ICT Regulations

Purpose of this document

The purpose of this document is to establish and communicate the policy and control measures for the use of ICT resources within The Hague University of Applied Sciences.

Purpose of the regulations

These regulations describe the rules for the use of the ICT Service Package. Its purpose is to guarantee a secure, reliable, and legally compliant ICT environment. These regulations apply to everyone who uses the ICT facilities of the University of Applied Sciences.

ICT facilities include:

- Email address and mailbox,
- Digital storage facilities
- Software and applications
- Computers, laptops, mobile devices and peripheral equipment belonging to the University of Applied Sciences
- Network facilities
- Lending of equipment and audiovisual resources
- Access to databases and digital learning environments

Every User is deemed to be familiar with and in agreement with these regulations and the obligations arising therefrom.

In this introduction you will find a top 10 of the most important rules that you must abide by. This does not alter the fact that you must be familiar with the entire ICT Regulations.

1. Use of Multi Factor Authentication (MFA) is mandatory and for that you need a cell phone with authentication app.
2. ICT resources provided by THUAS remain the property of THUAS.
3. Loss, theft and/or missing equipment of THUAS must be reported immediately to the iFrontoffice. In the event of theft, the User must also report this to the police.
4. In the event of a (suspected) data breach, a report must be made immediately to the Privacy Officer via iFrontoffice, Data Breach Report.
   Please do not report phishing and spam via iFrontoffice, but via the ‘Report’ button at the top of Outlook.
5. Employees are not permitted to store THUAS data on mobile data carriers, home computers or other unsecured equipment not provided by THUAS. Read more about the rules regarding storing and sharing data in Article 13.
6. All data created, collected and stored on THUAS ICT facilities are the property of THUAS unless specific arrangements have been made.
7. When the username of THUAS is used as a login to an external service, one is never allowed to utilise the same password as at The University of Applied Sciences (see the intranet for guidelines and tips regarding passwords).
8. It is not permitted to set up forwarding rules in the mail client from the ICT Services provided by the University of Applied Sciences to an external email address.
9. The User is responsible for the timely securing and transferring of e-mail messages and data before departure.
10. Follow the travel advice of the Ministry of Foreign Affairs regarding the use of business equipment abroad. For advice, please contact the End User Services team leader.
11. If lending equipment is returned late or incomplete, a fee will be charged, and the F&IT department may decide not to lend any more equipment to this person in the future. The availability of lending resources is not guaranteed.

Article 1. Definitions

The following terms used in these regulations are defined as follows:

a. *The University of Applied Sciences or THUAS:* The Hague University of Applied Sciences.
b. *Digital services:* Services offered by The University of Applied Sciences, including: a digital identity, email address and mailbox; digital storage facilities, digital library facilities, software and software licenses.
c. *ICT facilities:* facilities made available by The University of Applied Sciences, including the computer and network facilities deployed for the provision of these services comprising, among other things, the (fixed) workstations, the peripheral equipment, laptops, notebook computers, the fixed-line and wireless network infrastructure, the servers, the operating systems and software.
d. *Telephony*: the landline and mobile telephones and infrastructure provided by the Facilities & IT department (F&IT).
e. *Audiovisual equipment*: analogue and digital presentation equipment, both permanent and mobile photography, video and audio equipment, including accessories and flip charts.
f. *Digital identity*: a unique profile that gives the User access to (part of) digital services, through a combination of identifying and authorising attributes (for example: a Username and password).
g. *Multi Factor Authentication*: an additional attribute (e.g. a token via an authenticator app) to confirm the User's digital identity when accessing the system.
h. *ICT services package*: all resources, services and facilities listed under article 1.b through 1.g.
i. *Borrower*: the individual who borrows parts of the University's ICT services package for a given period.
j. *User*: anyone using the ICT services package.
k. *Staff member*: a person employed by The University of Applied Sciences.
l. *Student:* a person enrolled as a student or external candidate at The University of Applied Sciences, or a person who has applied for enrolment at The University of Applied Sciences.
m. *Third party*: a natural person, not a student or staff member, for example a visitor, guest User or staff member of a supplier/external service provider.
n. *Guest*: a visitor (on one of the campuses) or guest user whose use of the Services Package ICT is limited to guest access on Wi-Fi or in THUAS' online M365 environment.
o. Data breach: Unauthorised or unintended access to personal data caused by a breach of the security of these personal data. The unwanted destruction, loss, alteration, or disclosure of personal data as a result of such as this kind of breach also constitutes a Data Breach.

Article 2. Basis for and scope of the regulations

1. These regulations set out further rules concerning the use of the ICT services package. Each User is deemed to know and be in agreement with these regulations and the ensuing obligations.
2. In respect of students, these regulations form an integral part of Part 1 of the Student Charter, as referred to in article 7.59(5) of the WHW and provide rules concerning the smooth running of events as referred to in article 7.57h(1) of the WHW.
3. In respect of staff members, these regulations further implement Article E-1 of the Collective Employment Agreement for the higher professional education sector.
4. In respect of third parties, these regulations set out the conditions for using the ICT services package.
5. Further provisions concerning service provision, such as accessibility, rates and opening times, will be communicated through The University of Applied Sciences' usual communication channels.
6. These regulations have been drawn up under the responsibility of the Executive Board and delegated to the dean of Facilities & IT.

7. These regulations are partly based on the Information Security Policy & Privacy Policy of The University of Applied Sciences approved by the Executive Board.

Article 3. Right of use & duties of the User

1. The following persons are permitted to use the ICT services package:
    a. Students
    b. Staff members
    c. Third parties
2. When using the ICT services package, Users must be able to prove their identity by means of a legal and valid identity document.
3. The User may only use those ICT Facilities that are necessary for the execution of the job or following the study. Assessment of the need for use of and access to parts of the ICT Service Package is made by the mandated and responsible manager of The University of Applied Sciences.
4. Any User who detects any technical defects, vulnerabilities, or other flaws in (part of) the ICT services package must notify the Front Office of the F&IT service thereof as soon as possible.
5. Loss, and/or the disappearance of devices that belong to The University of Applied Sciences must immediately be reported to the municipality where you lost the device and report it to the Front Office of the F&IT department.
6. A (suspected) data breach must immediately be reported to the Privacy Officer iFrontofice, Data Breach Report. Please report phishing and spam via the 'Report' button at the top of Outlook.
7. Employees are required to complete awareness training courses on information security and privacy in Arda.
8. The User is not permitted to read, copy, modify, or delete email messages, chat messages, etc. intended for another User, unless they have explicitly been authorised to do so by the User to whom they are addressed.
9. If a User accidentally receives an email that is not intended for that User, the User is expected to notify the sender and delete the email. If personal data are contained in the incorrectly received email, this constitutes a data breach. The User and the recipient must immediately report this to the Privacy Officer via Front Office, Data Breach Report.
10. For internal communication purposes, the University of Applied Sciences only uses the email address provided by the University of Applied Sciences.
11. Employees are not permitted to publish or copy official communications and/or data externally in any way whatsoever, unless this arises from their established work or position (e.g. posts on social media).
12. It is not permitted to set up forwarding rules in the mail client from the ICT Services provided by the University of Applied Sciences to an external email address.
13. Communication from the University of Applied Sciences takes place via the email address provided by the University of Applied Sciences.
14. The email address provided by the University of Applied Sciences may not be used for private purposes.
15. The User is expected to be vigilant against fraudulent emails, website pop-ups, and other electronic messages that may contain harmful software or are intended to obtain the User's Digital Identity. If the User suspects that a message is not legitimate, they are required not to open the message/website and any attachments or hyperlinks and to report it as SPAM/Phishing via Report in Outlook.
16. In the event of deregistration, termination of employment, or similar termination of the relationship between the University of Applied Sciences and the User, access to the digital services will immediately be withdrawn. The User is responsible for backing up and transferring email messages and data in a timely manner before leaving the University of Applied Sciences.

Article 4. Method of use

1. The User is only permitted to use the services provided in the ICT services package for purposes arising from the User's activities or degree programme at the University.

2. The ICT services package may be used in accordance with the principles of reasonableness and fairness. The User is obliged to comply with the instructions given by or at the request of the F&IT Department and to follow these promptly. The User is furthermore required to exercise due care.
3. The User is not permitted to undertake or participate in activities that could undermine the integrity and continuity of the services provided in the ICT services package.
4. The User is not permitted to use the services provided in the ICT services package for acts or practices contrary to the law, public morals, public order and generally accepted social values and standards.
5. The User is not permitted to use services from the ICT services package with the obvious intention of causing nuisance or harm to third parties, such as a threats, harassment, obscenities, or software piracy.

Article 5. Digital identity

1. The User will receive from The University of Applied Sciences a unique digital identity (a User profile) to use the ICT facilities and digital services. Where necessary, the User will also be provided with a tool for Multi Factor Authentication.
2. The use of MFA (through an Authenticator app on the mobile phone) to access the ICT Facilities is mandatory for every User (except Third Parties). Every User must therefore have a mobile phone and is obliged to install the Authenticator app on it.
3. The Users may only use the ICT facilities and digital services with the digital identity provided to the User. The digital identity is strictly personal and non-transferable. Users must maintain strict confidentiality of their password (or similar attribute). Users must take all reasonable measures to protect their digital identity.
4. Users are responsible for everything made through the action of their Digital Identity.
5. Users must notify the Front Office as soon as possible if they suspect or establish that their digital identity, i.e. Username, password or Multi Factor Authentication tool has been misused.
6. Users are not permitted to appropriate and/or use the digital identity of other Users in any way or form whatsoever.
7. Users are not permitted to gain access to or use ICT facilities or data that are not intended for them, or for which they have not received authorisation from the F&IT department.
8. Upon de-registration, termination of employment or a similar end to the relationship between The University of Applied Sciences and the User, the digital identity will be deactivated.
9. The User is only permitted to log on with his/her university of applied sciences digital entity to services on the Internet with which THUAS has a business relationship, which are relevant to the study to be followed or which are relevant to the User within the execution of his/her job. When the User name of The University of Applied Sciences is used as login to an external service one is not allowed to utilise the same password as at The University of Applied Sciences (see the intranet for guidelines and tips on passwords).

Article 6. Applications and digital files

1. Users themselves are not permitted to install applications on The University of Applied Sciences' devices, unless prior written consent has been granted by or on behalf of the director of F&IT.
2. Users are not permitted to copy or make available to third parties applications or digital files of a confidential nature made available by the University, unless prior written consent has been granted by or on behalf of the director of F&IT.
3. Users must ensure they store and transfer all documents and information of THUAS in a responsible manner. Employees are not allowed to store data from The University of Applied Sciences on mobile data carriers, home computers or other unsecured equipment not provided by The University of Applied Sciences. Always use the by the University of Applied Sciences provided online storage such as OneDrive, Teams or SharePoint for this purpose.

Article 7. Computer and audiovisual equipment for students

1. There are various spaces at The University of Applied Sciences where students can use The University of Applied Sciences' computer and audiovisual equipment. The institution's house rules, as set out in Part 1 of the Student Charter, remain in full force in these spaces.
2. Computer and audiovisual equipment that belong to The University of Applied Sciences may only be used for the purpose of work or study activities associated with The University of Applied Sciences.
3. In addition to article 7.2, the following rules apply;
    a. it is not permitted to remove, relocate or modify any equipment whatsoever, including cables and furniture.
    b. It is allowed to use a designated cable to connect a personal laptop, smartphone or tablet to The University of Applied Sciences' computer or audiovisual equipment.
    c. Only the following equipment may be connected to The University of Applied Sciences' computer and audiovisual equipment: Data carriers to transfer personal or education-related data, headphones and ergonomic peripheral equipment, such as a mouse or keyboard that require no additional software.

Article 8. Network facilities

1. Users are not permitted to connect or activate active network components, such as hubs, routers, bridges, switches, or stations providing wireless access inside the institution's buildings.
2. Users are not permitted to disproportionately occupy the available network facilities, such to be determined at the discretion of the director of F&IT or a staff member designated by the director.
3. The User is not allowed to remove, damage or modify any of the network cables and/or network equipment installed by The University of Applied Sciences.

Article 9. Equipment on loan

1. Students, staff members and third parties may borrow equipment from the Front Office from FZIT.
2. The equipment loan procedure published on the Student and Staff Portals applies to equipment provided on loan. The General Terms and Conditions for the Loan of Equipment published on the Student and Staff Portals apply, a hard copy of which will be made available at the request of the individual borrowing the equipment. The equipment will not be provided on loan until such time as the borrower has concluded an equipment loan agreement with the institution.
3. The availability of lending equipment cannot be guaranteed.
4. A charge will apply if equipment is returned too late or is incomplete upon return, and the F&IT Department may decide not to lend any further equipment to the individual concerned in the future.
5. In the event the equipment is lost or damaged, the costs of repair or replacement will be charged to the borrower.

Article 10. Copyright

1. The use of services provided in the ICT services package resulting in the infringement of copyright or intellectual property is prohibited. This applies to making available information as well as the use of applications without a valid licence.
2. Any claims submitted to the University arising from the infringement of copyright or any other intellectual property may be recovered from the User concerned.
3. See also article E-7 from the CAO for the HBO and the memorandum on ownership of research publications adopted by the Executive Board.
4. The User is responsible for properly checking for possible copyright infringement when using tooling that generates output composed on the basis of artificial intelligence (e.g. ChatGPT).

Article 11. Liability

1. The User is deemed to know the risks involved in the digital or electromagnetic storage or transfer of information, such as the loss of data and unauthorised access by third parties.
2. The User is liable for any damage or losses arising from the use of or failure of services provided in the ICT services package through wilful intent, negligence, an imputable act or an omission, on the part of the User.
3. The University excludes all liability for the quality and availability of services provided in the ICT services package and for the information distributed through the services provided in the ICT services package.
4. The User shall be liable for any direct and indirect damage the User causes to the services provided in the ICT services package through wilful intent, negligence, an imputable act (including misuse) or an omission, and is required to pay the institution compensation for such damage.
5. The User indemnifies the institution against third-party claims arising from infringement of their rights, to the extent such infringement can be attributed to the User. Any damage will be recovered from the User causing the damage.

Article 12. Monitoring

1. General checks will be performed, including monitoring data and telephony, which will not infringe the User's right to privacy. The purpose of such checks is to prevent control or capacity problems as well as inappropriate or unlawful use.
2. Should it emerge that a User is acting in breach of these regulations, or if there is evidence thereof, such as complaints, reports and system failures, the data of the User concerned may be examined, used and stored by or on behalf of the Executive Board as long as required for the purpose of further investigation and any measures to be imposed.
3. Within the Microsoft 365 platform, data is collected on the User's use of the Microsoft 365 services. The personal use is applied only for dashboards and insights that are shown only to the User. Anonymised usage is applied for various analyses within the platform.

Article 13 Privacy/GDPR in relation to the ICT Regulations

In the digital age, privacy plays a crucial role at the University of Applied Sciences. Users make daily use of ICT systems that process personal data and confidential information. In order to guarantee the privacy of all parties involved and to protect personal data, the ICT Regulations of the University of Applied Sciences are closely linked to the GDPR (General Data Protection Regulation). The GDPR has been in force since 25 May 2018 and imposes strict requirements on the processing of personal data.

1. **Personal data** are data that say something about a specific person and from which you can deduce who the person concerned is. Individual data that can be aggregated and thus say something about a particular person are also personal data.
2. **Processing** is a broad term and encompasses all actions that the University of Applied Sciences may perform with personal data. This varies from collecting, storing, and modifying to destroying data. Examples include storing student data, forwarding an email containing personal information, or consulting files containing personal data.
3. The Hague University of Applied Sciences processes a large amount of personal data, such as:
   a. student data (name, address, email address, marks, feedback, etc.);
   b. employee data (contract information, payroll administration, personnel administration, leave and absenteeism data, etc.);
   c. digital activities (logging into systems, using email and the internet);
   d. visual and audio material (photos/videos at events, etc.).
4. More information about the careful and secure handling of personal data can be found on the intranet page Privacy/GDPR.
5. **Ensuring the protection of personal data**

a. The University of Applied Sciences processes personal data in accordance with the GDPR and other relevant privacy legislation.
b. Users may only process personal data when necessary for study, education or research and in compliance with the rules of the GDPR.
c. It is **not permitted** to share personal data with third parties without the consent of the data subjects, unless there is a legal obligation or legitimate interest (valid legal basis).
d. It is **not permitted** to use personal data or confidential business information in GenAI tools, whether it belongs to the University of Applied Sciences, internship or graduation companies, relations where projects or assignments are carried out, or cooperation partners. According to the GDPR, any processing of personal data must be based on a valid legal basis. There is no valid basis for processing personal data in GenAI tools (not even with consent).
e. Email and other means of communication should not be used to send sensitive personal data without appropriate security measures in place:
    a. internal: share your file via Teams or SharePoint with the recipient (preferred) or email it to a THUAS email address
    b. external: send your file via SURFfilesender WITH a password. Send the password in a separate email to the recipient. Please do **not** use WeTransfer.
f. Data breach notification requirement: if you suspect a data breach, you must immediately report it to the Privacy Officer via iFrontOffice, Data Breach Report.
g. The University of Applied Sciences takes technical and organisational measures to ensure the confidentiality, integrity, and availability of personal data.
h. Access to personal data must be restricted to only those employees who need it for their job.

6. Access to systems

a. In accordance with Article 5.8, access to the ICT systems of the University of Applied Sciences is terminated at the end of the agreement as soon as an employee terminates their employment or a student terminates their enrolment in the degree programme. This process is important for protecting the data of the people involved and the overall security of the systems of the University of Applied Sciences.
b. Termination of employee access:
    i. When an employee terminates their employment (whether voluntarily or involuntarily), access to all ICT systems of the University of Applied Sciences, including email, network access and cloud services, is blocked. This also applies to external employees such as interns and consultants whose agreemeents are ending. The digital identity is deactivated.
    ii. Transfer of data: before access is revoked, the employee is obliged to transfer all necessary documents stored on the systems of the University of Applied Sciences to the authorised person, for example the manager or an employee designated by the manager. The files must be transferred carefully and securely via a folder in Teams/SharePoint containing the relevant documents, with the departing employee granting access to their manager or a designated colleague from the department.
c. Termination of student access:
    i. When a student is deregistered, access to all ICT systems of the University of Applied Sciences, including email, network access and cloud services, is blocked. The digital identity is deactivated.
    ii. Transfer of data: students who terminate their studies must ensure that all necessary documents are transferred from OneDrive and their mailbox before deregistering.

7. Data storage

The following applies to the storage of data on the ICT facilities of the University of Applied Sciences:

a. Each User is provided with a personal storage location: OneDrive (in Microsoft 365). This is a personal location. This is where a User stores files and data that only they need for the performance of their duties or that are not yet ready to be shared with others. The personal storage location is expressly **not** intended for the **permanent** storage of work-related files containing personal data. Personal data may not be retained longer than necessary for the purpose for which they were collected.
b. Every User can become an owner of and/or be added to Teams in Microsoft Teams. Teams are, by definition, intended for collaboration. All members of the team automatically become owners of all data posted within the Team (some nuances are possible). A Team offers

possibilities such as sharing data, co-creating data, jointly processing and enriching data. In addition, a Team offers simple forms of collaboration through chat, messaging, channels and meetings, among other things.

c. The University of Applied Sciences provides SharePoint Online Sites that are primarily intended for publishing data to larger groups or supporting business processes.
d. The aforementioned SharePoint Online Sites and public data can be communicated and published via the Intranet.

8. Information storage

The following applies to sharing information outside the University of Applied Sciences:

a. Only data that are suitable for this purpose may be shared (e.g. by email) with external recipients. Data of a confidential/strictly confidential nature may only be shared outside the organisation in a secure manner (see the F&IT Intranet for options).
b. Within the online Microsoft 365 environment of the University of Applied Sciences, you can collaborate with external parties by sharing a file from OneDrive / Teams/SharePoint Online with them or adding them as a Guest to a Team or SharePoint site. Users should exercise caution when inviting external parties.
c. Guest invitations that are not used will be withdrawn after 30 days.
d. A Guest who has not participated in the relevant collaboration platform (Teams, SharePoint Online) for 180 days will be removed.
e. Owners are responsible for reviewing the need for external access to their Teams or SharePoint Online Site on a quarterly basis and adjusting it as necessary.

Article 14. Violation

1. In the event a student breaches any provision of these regulations or acts in contravention of the equipment loan agreement or the General Terms and Conditions for the Loan of Equipment, the Dean of Faculty or Director of Services concerned may take measures as described in the Code of Conduct and Disciplinary Measures at the request of the director of F&IT or otherwise. In addition to the above, the student may be denied access to and use of the services provided in the ICT services package for a maximum period of one year.
2. If a staff member violates these regulations or acts in contravention of the equipment loan agreement or the General Terms and Conditions for the Loan of Equipment, this may imply that the staff member has not acted as befits a good staff member within the meaning of article E- 1 of the Collective Employment Agreement for the higher professional education sector. In that case the Executive Board may take a disciplinary measure against the staff member concerned within the meaning of article P-3 of the Collective Employment Agreement for the higher professional education sector.
3. The breach of these regulations or acting in contravention of these regulations by a third party may result in the imposition of sanctions on said third party by the director of F&IT.
4. In the event of a severe breach of these regulations and in case of an emergency, the director of F&IT (or a designated security staff member) may take immediate measures to stop the violation, in addition to the measures referred to in paragraphs 1 and 2. The director of F&IT will notify the Faculty Director concerned, leading lector or the Director of Services, as well as the Executive Board, of the measure taken without delay.

Article 15. Reporting to the police and judicial authorities

If a criminal offence has been committed, the University will report the offence to the police or judicial authorities, in addition to taking the measures described in article 14. Details of the User may be given to the police or judicial authorities if they formally request these as part of an investigation of criminal offences.

Article 16. Complaints

In the event of complaints or observed acts contravening these regulations, any individual may contact the director of F&IT or an officer designated by the director of F&IT. Correspondence concerning the above will be treated as confidential.

Article 17. Legal protection

1. A student may lodge an objection against a decision as referred to in article 14(1) with the Legal Protection Desk within six weeks. The period takes effect the day after the decision has been communicated to the student either in writing or by email.
2. A staff member may lodge an appeal against a decision as referred to in article 14(2) with the Subdistrict Court or the Appeals Board for the Higher Professional Education Sector in Utrecht, depending on the measure. The notice of appeal must be submitted within six weeks starting from the day on which the decision against which the appeal was lodged was sent or issued to the staff member.

Article 18. Final provisions

1. These regulations may be referred to as 'ICT Regulations'.
2. In the event of situations for which this regulation does not make provisions, the Executive Board will decide.
3. The Executive Board will ensure that these Regulations are evaluated regularly.
4. This evaluation will take place at least once every 3 years. Amendments to these Regulations will be announced through THUAS messages and the most recent version is published on the intranet page of The University of Applied Sciences.

May 2025