[Regulations governing the use of Internet and ICT facilities by employees - 2020]

These Regulations were adopted by the Executive Board on [DATE].

These Regulations were approved by the Executive Board on [DATE].

The University Council endorsed these Regulations on [DATE].

The EUR consultative body for staff matters EUROPA endorsed these regulations on [DATE].

These Regulations shall enter into force on [**DATUM**].

Contents

Chapter I – General

The use of internet and ICT resources is necessary for many Jobholders at Erasmus University Rotterdam (EUR) to properly perform their duties. However, the risks for EUR associated with the use of these facilities necessitates drawing up a code of conduct. Given the context of such risks, the Jobholder is expected to make use of the internet and ICT facilities in a responsible manner.

In these Regulations, EUR has set out the rules regarding the use of these company resources. The objective of these rules is to find an equitable balance between the safe and responsible use of ICT and internet and the Jobholder's privacy.

Pursuant to legislation, EUR's position as an employer authorises the organisation to set rules for how work is to be performed and for maintaining good order in the workplace. In addition to its statutory basis, these Regulations are also based on the Collective Labour Agreement Dutch Universities (CAO NU).

Article 1.1 – Definitions

1. The following terms and definitions are used in these Regulations:
   - *Awb:* The Dutch General Administrative Law Act;
   - *BBR-EUR*: The applicable Administration and Management Regulations, as described in Article 9 subsection 4 of the Higher Education and Research Act;
   - *Board* The EUR Executive Board;
   - *BW:* Dutch Civil Code;
   - *Confidential position*: A Jobholder with a recognisable position involving confidentiality, such as a confidential counsellor, ombudsman, company doctor, HR-advisor or other position that can invoke confidentiality under the law;
   - *Course Participant* the person enrolled in a programme, course or module at EUR, which does not fall under the scope of Article 7.3 and Article 7.3a of the Higher Education and Research Act;
   - *DPO:* Data protection officer. The person appointed pursuant to the regulations in the GDPR to monitor the application and compliance with the GDPR;
   - *EUR:* Erasmus University Rotterdam;
   - *EUR data:* Data created, compiled, enriched or structured by any other means by the Jobholder by reason of his/her employment agreement and/or the activities that could reasonably be considered part of the work tasks, such as teaching, research, or business operations. EUR data falls under the scope of the Collective Labour Agreement Dutch Universities (Intellectual property rights);
   - *EURnet:* The cabled and wireless network infrastructure as offered by EUR;
   - *GDPR:* General Data Protection Regulation;

- *ICT Facilities:*	Communications, computer and networking facilities at EUR, including telephone facilities, EURnet facilities together with all the associated equipment and software, connections with other networks such as the Internet, computer and audiovisual facilities – either linked to EURnet or otherwise – in halls and rooms at EUR, as well as ICT services offered to Jobholders;
- *In writing*:	In writing or 'by electronic means', as described in Article 6:227a of the Dutch Civil Code.
- *Jobholder:*	This term refers to a member of Staff or a person who is in possession of a valid Hospitality Agreement;
- *Management*:	The entirety of decisions, operations and activities with which the Executive Board implements University policy regarding the acquisition and allocation of financial resources, the purchase, care and maintenance of tangible resources, the deployment of Staff, and the efficient and legitimate use of the aforesaid, as described in Article 1.1, paragraph 1 of the BBR-EUR;
- *Manager*:	The person charged with performance of management duties on the Executive Board's instructions, in its name and under its responsibility;
- *Regulations:*	Regulations governing the use of Internet and ICT facilities by employees - 2020;
- *Staff*:	Persons employed by EUR or seconded elsewhere on assignment;
- *Student:*	A persons who is enrolled at EUR for an initial programme offered by EUR, and who makes use of EUR's course and examination facilities. This includes persons enrolled as external candidates and, in the framework of the Regulations, Course Participants;
- *Targeted investigations:*	Investigations in which traffic, traffic data or EUR data is made accessible for inspection as a result of reasonable and well-founded suspicion of a breach of these Regulations;
- *WHW:*	The Higher Education and Research Act.

2. The terms used in these Regulations have the same meaning as those in the WHW if such terms also occur in the WHW and have not been included in the definitions.
3. Use of the masculine form in these Regulations can also be understood to mean the feminine form and vice versa.
4. Use of a term in singular form in these Regulations can also be understood to mean plural and vice versa.

Chapter II – Guiding principles

Article 2.1 – Purpose of these Regulations

These Regulations set out rules with respect to the use of ICT and internet company resources by EUR Jobholders. These rules aim at:

1. safeguarding the network and system, including protection from damage and misuse;
2. combating sexual harassment, discrimination and other criminal offences;
3. protecting EUR's confidential information and intellectual property;
4. protecting the personal data of Jobholders, of Students and their parents, of alumni, of participants in scientific research, and of other clients and visitors;
5. preventing negative publicity; and
6. cost and capacity management.

Article 2.2 – Private use

Limited private use of internet and ICT resources is permitted within reasonable limits, provided that it does not disrupt daily work activities or EUR's network, or, as the case may be, lead to disproportionate costs for EUR. In this regard, refer also to the provisions in Article 4.1 and Article 5.1, paragraph 3.

Article 2.3 – Scope

These Regulations apply to all Jobholders.

Article 2.4 – The Jobholder's privacy

In the context of upholding these Regulations, EUR will take all possible measures to limit access to privacy-sensitive information or personal data of individual Jobholders. Where possible, EUR will use only automated monitoring and filters, without providing insight into individual behaviour to the organisation or third parties.

Article 2.5 – Prohibited use

It is prohibited to use computer, network and ICT communication facilities provided by EUR for purposes that are in breach of law or regulations, damaging to EUR's image, a risk to the safety of others, or, unless required for execution of tasks assigned by EUR, conflict with the generally accepted standards of conduct.

Examples (thus non-exhaustive) of prohibited use are:

1. processing and/or sending personal data in a manner that is in breach of the GDPR;
2. sending and/or posting messages with pornographic, racist, discriminatory, threatening, insulting and/or offensive content;
3. sending unsolicited messages to large numbers of recipients insofar as this does not arise from assigned tasks, sending chain letters, or sending malicious software such as viruses, Trojan horses or spyware.

Chapter III – Handling confidential information

Article 3.1 – Confidentiality

Jobholders must ensure strict confidentiality in handling confidential information and take adequate measures to preserve confidentiality.[1]

Article 3.2 – Theft or loss

The Jobholder is required to immediately report theft or loss of equipment containing EUR data, and in cases where it is technically feasible to do so, cooperate in the deletion of EUR data contained on the equipment. Deletion of data on equipment owned by EUR will be executed without any further intervention by the Jobholder.

Chapter IV – Use of computer and network facilities

Article 4.1 – Private use

1. Computer and network facilities are made available to be used by the Jobholder in the context of the Jobholder's job role. Use is therefore associated with tasks resulting from this job role. Private use is only permitted as stipulated in Article 2.2 of these Regulations;
2. In principle, saving private files or information on EUR systems is not permitted, unless such limited use does not disrupt daily work activities or EUR's network, or leads to disproportionate costs for EUR.

Article 4.2 – Stipulated systems

EUR may stipulate the use of systems or applications for teaching, research or other business purposes, such as an electronic learning environment, an e-mail system, or multimedia services. When performing work tasks, the Jobholder is required to use stipulated systems or applications and strictly comply with the associated requirements and restrictions.

Article 4.3 – Complying with directives and instructions

The Jobholder is required to comply with general instructions issued by or on behalf of EUR regarding the use of ICT facilities. When using ICT facilities, instructions and directives issued by the IT department must be complied with immediately. EUR may impose additional conditions and rules related to the use of communication, computer and network facilities.

Article 4.4 – Connecting to EURnet – installing software

1. Installing software on EUR's computer and network facilities or altering or modifying these facilities is not permitted without consent from the IT department. It is also prohibited to connect servers and active network components (such as access points and routers) without the consent of the IT department. This consent may be subject to additional conditions. The Jobholder is required to comply with these additional conditions.

[1] If there are any questions or ambiguities, the Jobholder will contact his manager or employer.

2. Connecting personal devices (such as laptops, tablets and telephones) at EUR locations is only permitted on the (wireless) network connections made available for this purpose. Access to these connections is subject to rules, such as the mandatory installation of a virus scanner, regularly updating the operating system, and using encryption and password protection.
3. The use of EUR's Computer and network facilities using personal devices or EUR devices from locations outside of EUR locations is only permitted through secure (Wi-Fi) networks or secure access made available for this purpose (such as VPN or Virtual desktop), provided that these devices meet additional conditions, such as the installation of a virus scanner, regularly updating the operating system, and using encryption and password protection.

Article 4.5 – Explicit Prohibitions

With respect to the use of communication, computer and network facilities, the Jobholder is in any case prohibited from:

1. Gaining access or attempting to gain access to the data of other users and to program files of computer systems, or altering or destroying them, if the aforementioned activities do not form part of the duties assigned by EUR;
2. Gaining access or attempting to gain access to computer systems if this involves systems where no explicit means of access has been created for the Jobholder;
3. Taking any action that undermines the integrity and availability of the facilities;
4. Making attempts to obtain higher privileges for the facilities than those that have been granted;
5. Making attempts to obtain system or user authorisation codes (such as passwords) belonging to others/third parties in any way and in any form;
6. Reading, copying, altering or erasing e-mails and other messages intended for others, unless authorisation has been granted for this purpose by the other party involved within the settings of the e-mail system;
7. Copying the software, data files and documentation made available by EUR, or giving third parties access to them, unless given consent to do so in writing by the Manager;
8. Intentionally, or through culpable acts or omissions, introducing "malware" to or via ICT facilities.

Article 4.6 – Acting with due care when using means of authentication

The Jobholder is required to exercise due care with the provided personal login details and any other additional means of authentication (such as smart cards and tokens). It is not permitted to share personal passwords and additional means of authentication. In cases of suspected abuse of a password, the IT department may immediately block access to the associated account.

Chapter V – Use of e-mail and other ICT communication tools

Article 5.1 – E-mail

1. The e-mail system and the associated mailbox and e-mail address are made available to the Jobholder in the context of his job role. Use is therefore associated with tasks resulting from this job role. Private use of the e-mail account is only permitted under the provisions in Article 2.2.
2. In the context of performing his work activities for EUR, the Jobholder is required to use EUR's e-mail facilities for sending and receiving e-mails. Copying, moving, or forwarding these messages (by automated or other means) to e-mail systems and accounts not provided by EUR is prohibited.
3. When sending private e-mail messages, it is preferable that the Jobholder does not use the e-mail address provided by EUR. In this regard, see also the provisions in Article 2.2

Article 5.2 – Access to the mailbox in cases involving compelling business interests

In cases of illness or an unexpected long-term absence of the Jobholder, and only if there is a compelling reason involving business interests to obtain access, EUR is entitled to give a substitute or manager access to the Jobholder's files or mailbox, but only after separate permission has been obtained from the Jobholder's manager. However, this does not include access to any folders marked as private or e-mails that are recognisable as private, or e-mails sent to or received from a person holding a Confidentiality position. If the Jobholder has not made any such designations, EUR can ask a confidential counsellor to check the Jobholder's information, identify any private information, and place it in a separate folder before the substitute or manager is given access.

Article 5.3 – Blocking access to communication channels

EUR reserves the right to restrict access to certain communication channels, such as telephone numbers, URLs and IP addresses.

Article 5.4 – Registration of mobile devices

1. The use of telephones, tablets and laptops made available by EUR will be recorded. This registration takes place in the context of charging the costs associated with data and telephone usage within the EUR organisation, and to safeguard the management, continuity, integrity and availability of technical infrastructure or services. In this registration, the content of telephone conversations will not be recorded.
2. In cases of unusually high costs, EUR reserves the right to verify the usage of the subscription. For each subscription, lists of numbers, the duration of calls placed and the amount of data sent can be retrieved for this purpose. Based on the results, further investigation may be conducted as described in Chapter 7 of these regulations.

Chapter VI – Monitoring and verification

Article 6.1 – Monitoring and verification

Monitoring the use of ICT facilities and internet usage will only take place in the context of enforcing the rules in these Regulations for the purposes stated in Article 2.1.

1. For the purpose of verifying compliance with the rules, data will be collected in an automated manner (logging) under the responsibility of the IT service director. Only authorised Jobholders of the IT department will have access to this data, and this data is made available only in a pseudonymised format to the IT service director. If so decided by the IT service director, the data can also be made available to other managers and persons responsible. The IT service director may decide to take additional technical measures.
2. All possible measures will be taken to use technical means to ensure prohibited use of ICT facilities is rendered impossible. When granting access to EURnet, ICT facilities and/or EUR data, the use of security software and security measures may be required for the devices used. This also includes software that makes it possible to verify the effectiveness of these measures prior to granting the desired access.
3. If there is a reasonable and well-founded suspicion of violation of the rules by a Jobholder, e-mail and internet use may be monitored at the level of individual traffic and traffic data (Targeted investigation, see Chapter 7). Inspection of content will be done only for compelling reasons.
4. When obtaining access at the level of personal data and/or traffic and traffic data, EUR will fully adhere to the GDPR and other relevant legislation and regulations.

Chapter VII – Investigations and Targeted investigations

Article 7.1 – Investigations

Investigations into the security or integrity of peripheral equipment and systems usage is conducted by the IT service based on concrete indications. The results of the investigation are shared only with the Jobholder in question, for the purpose of improving the security or integrity of the peripheral equipment.

Article 7.2 – Procedure for Targeted investigations

A Targeted investigation is only conducted once instructions in Writing are issued by the Board, and the investigation is conducted in a manner that minimises the invasion of privacy of the person or persons involved.

Prior to issuing such instructions, the Board will in any case take the following into consideration:

1. If the subject of the intended Targeted investigation is a person in a Confidential position, the Board will ask the DPO to make an additional assessment in relation to the privacy rights of Jobholders and/or students whose data has been processed by the person under investigation. This assessment may result in an adjustment of the Targeted investigation.

2. If a case is made for an intended Targeted investigation as a result of a reasonable and well-founded suspicion of a breach of these Regulations, but without a reasonable or well-founded suspicion that criminal offences have been committed within the meaning of the Criminal Code or other statutory provisions, then the Board will consult with the central EUR confidential counsellor regarding the intended investigation.
3. In all other cases, the Board can order a Targeted investigation if there is a reasonable and well-founded suspicion that these Regulations have been breached.

If the investigation does not give rise to further measures, the records will be promptly destroyed.

Article 7.3 – Information about the Targeted investigation

The Jobholder will be informed in writing by the Manager as soon as possible of the reason for the Targeted investigation, its procedure and its outcome. The Jobholder will be given an opportunity to provide an explanation of the data found. A delay in informing the Jobholder is permissible only if there is a compelling reason to do so.

Article 7.4 – Safeguarding private accounts and equipment

EUR's IT service Jobholders and EUR's security organisation may only gain access to the private accounts or private equipment of Jobholders if the Jobholder has given his consent.

Chapter VIII – Measures

Article 8.1 – Measures

1. When these Regulations or general statutory regulations are violated, the Executive Board may take disciplinary measures, depending on the nature and severity of the violation. Examples of such measures include a warning, a reprimand, a transfer, suspension, or termination of employment. The Board may also decide to impose a temporary or long-term measure restricting access to certain ICT facilities.
2. Disciplinary measures cannot be taken based solely on automated processing.
3. Contrary to the provisions in paragraphs 1 and 2, it is possible that EUR may implement a temporary block on a facility following (automated) observation of disruptive activity. This block will be maintained until it is demonstrated that the cause has been removed. If the cause recurs, disciplinary measures may be taken.

Chapter IX - Concluding provisions and transitional provisions

Article 9.1 – Interpretation

In cases relating to matters provided for in these Regulations that are not covered by these Regulations, or in cases where these Regulations may be interpreted in several ways, the decision shall rest with the Executive Board.

Article 9.2 – Management of these Regulations

These Regulations are under the management of the IT service director.

Article 9.3 – Translation

If there are any inconsistencies between a translation of these Regulations and the Dutch version, the Dutch version shall prevail.

Article 9.4 – Publication

The Board will publish these Regulations on the EUR website.

Article 9.5 – Entry into force

These Regulations shall enter into force following endorsement by the University Council and approval by EUROPA, at a time yet to be determined by the Board.

Article 9.6 – Abbreviated title

1. These Regulations shall be cited as: Regulations governing the use of Internet and ICT facilities by employees - 2020.

Article 9.7 – Applicable law

1. These Regulations are governed exclusively by Dutch law.

Article 9.8 – Withdrawal

1. The Regulations governing the use of Internet and ICT facilities by employees - 2015 will be withdrawn effective [**DATE**].