VU VRIJE UNIVERSITEIT AMSTERDAM

ICT FACILITIES REGULATIONS FOR STAFF OF VRIJE UNIVERSITEIT AMSTERDAM

Version 1.4

VU VRIJE UNIVERSITEIT AMSTERDAM

IS VERDER KIJKEN

ICT Facilities Regulations for Staff of VU Amsterdam

Contents

CHAPTER 1. INTRODUCTION

Vrije Universiteit Amsterdam (hereinafter: **VU Amsterdam**) gives its staff access to its ICT facilities, including computers, the internet, e-mail and other applications. It is extremely important that staff members use the ICT facilities safely and responsibly.

These 'ICT Facilities Regulations for Staff of VU Amsterdam' (hereinafter: **Regulations**) describe which rules of conduct apply to the use of ICT facilities by VU staff. The Regulations are intended to clarify VU Amsterdam's interpretation of 'safe and responsible use', and its expectations regarding conduct of its staff. The purpose is as follows:

- ensuring the confidentiality, integrity and availability of the ICT facilities[1];
- keeping the costs manageable for VU Amsterdam; and
- ensuring that the rights and reputation of VU Amsterdam and others are not violated.

In addition, these Regulations explain how VU Amsterdam monitors its ICT facilities. VU Amsterdam ensures there is a sound balance between reaching the aforementioned objectives on the one hand, and the right to privacy of its staff members on the other hand.

Logging and monitoring play a vital role in monitoring the ICT facilities. Logging and monitoring are automated processes and in principle are not geared towards individual staff members. Investigations into individual employees are only possible if there is a justified suspicion of a breach of the rules of conduct or other seriously culpable conduct. The starting point for targeted investigation is that only Traffic Data – also known as metadata – is investigated and not the content of files or messages. Only in the case of compelling reasons and when deemed necessary is it possible for substantive data of individual staff members to be investigated. These Regulations define the conditions under which targeted and substantive investigation is possible. They also describe for which other purposes Traffic Data is used.

Finally, these Regulations state how supervision on compliance with these Regulations has been organized and which final provisions apply.

CHAPTER 2. GENERAL PROVISIONS

Article 1. Glossary

a. **Acceptable use**: use of the ICT facilities, whose confidentiality, integrity and availability are ensured and whose costs are manageable while not violating the rights and reputation of VU Amsterdam or third parties.
b. **Authorized Officer**: a Staff Member who, owing to their position, has been authorized by VU Amsterdam to have access to certain data that is collected by means of Logging and/or Monitoring.
c. **Executive Board**: the Executive Board of VU Amsterdam.
d. **Data Breach**: a security breach that inadvertently or unlawfully leads to the corruption, loss, amendment or unauthorized issuance of or the unauthorized access to forwarded, stored or differently processed personal data, within the meaning of Article 4.12 of the General Data Protection Regulation (GDPR).

[1] These terms are derived from the information security domain and entail that systems and the information in these systems are accessible (availability), reliable (integrity) and can only be consulted by the appropriate people (confidentiality).

e. **Data Protection Officer (DPO)**: an internal officer within the meaning of Article 37 ff. of the General Data Protection Regulation (GDPR). The DPO independently monitors compliance with the laws and regulations pertaining to data protection and the VU Amsterdam policy as regards the protection of personal data.
f. **Code of conduct**: the rules as contained in chapter 3 of these Regulations.
g. **Targeted investigation**: an investigation into an individual Staff Member or group of Staff Members, making use of the Traffic Data that relates to the Staff Member or Staff Members.
h. **ICT facilities**: all facilities used and made available by VU Amsterdam in the context of its information and communication processes. These facilities may be made available by VU Amsterdam or through contracted third parties. These facilities include: networks, the internet, computers, programs and applications, printers, copiers and scanners, information carriers, storage space, e-mail, mobile and other phones and other means of communication.
i. **Substantive investigation**: an investigation into an individual Staff Member or group of Staff Members, not only making use of the Traffic Data that relates to the Staff Member or Staff Members, but also studying the content of files or messages of the individual Staff Member or Staff Members.
j. **Logging**: automatically recording Traffic Data.
k. **Staff Member**: persons with an employment contract with VU Amsterdam, persons working under the authority and/or responsibility of VU Amsterdam without an employment contract, including temporary employees, seconded employees, independent contractors, trainees, fellows, visiting lecturers and/or researchers, as well as other persons who perform work for the benefit of VU Amsterdam, which involves them using ICT facilities.
l. **Monitoring**: automatically collecting and analysing Traffic Data. Monitoring takes place based on general parameters and patterns and is not focused on individual Staff Members.
m. **Traffic Data**: all data relating to or ensuing from the use of ICT facilities which do not concern the content of files or messages. Traffic Data are also referred to as metadata in the context of ICT facilities.

Article 2. Scope

2.1 These Regulations apply to any use of the ICT facilities by Staff Members, regardless of the nature of the use, i.e. business or personal, and regardless of the manner of use.
2.2 In addition to these Regulations, VU Amsterdam may set special conditions to the use of specific or general ICT facilities by certain or all Staff Members (hereinafter: **Special Conditions**).

Article 3. Objective

3.1 The purpose of these Regulations is to:
a. promote and enforce the Acceptable use of ICT facilities by Staff Members; and
b. establish the normative framework for handling data that (may be) stored in the context of the use of ICT facilities.

CHAPTER 3. CODE OF CONDUCT

Article 4. Rules of conduct

4.1 Staff Members make careful use of the ICT facilities and act in accordance with the instructions issued by VU Amsterdam.
4.2 When using the ICT facilities, Staff Members abide by the applicable laws and regulations, these Regulations and Special Conditions, if applicable.
4.3 Staff Members respect the security measures.

4.4 Staff Members prevent incorrect or unauthorized use of ICT facilities and act as good employees. Where possible, VU Amsterdam ensures that incorrect and unauthorized use is rendered technologically impossible.
4.5 Staff Members prevent the rights and reputation of VU Amsterdam from being violated.
4.6 Staff Members handle their login details carefully and refrain from issuing them to third parties.
4.7 Staff Members refrain from providing access to the ICT facilities to third parties[2] nor loan them out.
4.8 Staff Members respect the intellectual property rights of VU Amsterdam and of third parties.
4.9 Staff Members handle confidential information, including personal data to which they have access in the context of their position, in a strictly confidential manner.

Article 5. Unauthorized use

5.1 The following acts are deemed to be unauthorized use of the ICT facilities:
a. disrupting, damaging, hindering, retarding or otherwise influencing the intended confidentiality, integrity and availability of the ICT facilities;
b. intentionally spreading or promoting the spreading of viruses, Trojans, spyware, malware or other harmful software;
c. intentionally spreading or promoting the spreading of messages for commercial purposes, unsolicited or otherwise;
d. circumventing security measures;
e. intentionally obtaining or granting higher privileges or access rights – or attempting this – than required for the performance of the work;
f. assuming a false capacity or identity;
g. intentionally having or making available or copying material protected by copyright or another type of intellectual property right without the permission of the title-holder or title-holders, including illegal, forged or stolen versions of software;
h. any use of the ICT facilities leading to the discrimination, sexual or other intimidation or threatening of others;
i. intentionally visiting websites containing pornographic, racist or otherwise discriminating material, placing such material – or having it placed – on or in the ICT facilities, unless this is required in the context of the job performance of the Staff Member;
j. intentionally storing, spreading or otherwise processing material whose possession is punishable; and
k. intentional unauthorized publicizing of personal data or other confidential data of VU Amsterdam – or having it publicized.

Article 6. Business and personal use

6.1 VU Amsterdam makes its ICT facilities available to Staff Members for the performance of their tasks and duties for the benefit of VU Amsterdam. The ICT facilities are thereby primarily intended for business use.
6.2 Limited personal use of the ICT facilities within the parameters as laid down in these Regulations is allowed, provided that:
a. this takes place within the boundaries of reasonableness;
b. the work performance of the Staff Member is not hindered;
c. the use of ICT facilities by or the work of other Staff Members is not hindered;

[2] An exception is the situation in which it is the duty of a Staff Member to grant access to the ICT facilities to other Staff Members.

d. this does not create an unreasonable technological or financial burden on the ICT facilities of VU Amsterdam; and
e. this is not done for commercial purposes.

6.3 Staff Members ensure that files and messages that are personal are marked as 'personal'.

6.4 Staff Members are aware that VU Amsterdam may need to grant another Staff Member access to their personal storage space or mailbox.[3] For instance, when a Staff Member is absent for a prolonged period of time or no longer works at VU Amsterdam. Files and messages that are marked 'personal', as referred to in article 6.3, are disregarded in this matter. The same applies to privileged information within the meaning of article 10.3 (e). Access to the sections of the personal storage space or mailbox that are relevant for work handover is only possible when:
a. this is proportionate, considering the intended objective of the access;
b. no reasonable alternative is available;
c. this is not contrary to a duty of confidentiality or duty of secrecy of a Staff Member, within the meaning of article 10.3 (b), (c) or (d); and
d. written consent has been obtained from the Faculty Director of Operations or the Director of the Service Department where the Staff Member concerned works. If the Staff Member concerned is a dean, Director of Operations or Director of a Service Department, permission must be obtained from the Executive Board. If the Staff Member concerned is a member of the Executive Board, permission must be obtained from the VU Amsterdam Supervisory Board.

Article 7. Incident reporting

7.1 Staff Members promptly report incidents pertaining to ICT facilities to the IT Service Desk via servicedesk.it@vu.nl or 020-5980000.

7.2 'Incidents' shall in any case include (a suspicion of):
a. loss or theft of login details;
b. loss or theft of ICT facilities, such as a computer, telephone or USB drive;
c. unauthorized access to ICT facilities;
d. unauthorized or unintentional corruption, publication or amendment of or unintentional access to personal data or otherwise confidential or sensitive business or research data;
e. the presence of harmful software, including a virus, Trojan, spyware, malware; or
f. a phishing attack.

CHAPTER 4. LOGGING AND MONITORING

Article 8. Logging

8.1 When using ICT facilities, Staff Members must be aware of the fact that certain data, including personal data, may be recorded. In some cases, this is an intentional, well-founded choice and in other cases this is borne from a technical-functional need or inevitability.

8.2 VU Amsterdam shall endeavour to minimize both the number of categories and the total amount of data collected in the context of the use of ICT facilities. The data collected are anonymized or pseudonymized as much as possible.

[3] Staff Members are expected to store work-related files and messages on locations that are accessible to colleagues – direct or indirect – such as the G drive, wherever possible. This way, work handover in case of long-term or other absence from work is possible without the need for the colleague to have access to the personal storage space or mailbox of the Staff Member who is absent.

8.3 The following incidents are always logged[4]:
a. acts of Staff Members, such as login attempts, system access, e-mail use, telephone use, access to files and website visits;
b. the use of technical management functionalities, such as changing the configuration or settings, executing a system command, starting and stopping services, executing a back-up or restore;
c. the use of functionalities for functional management, such as changing the configuration and settings, release of new functionalities, interventions in data sets, including databases;
d. acts in security management, such as provisioning and deprovisioning users, awarding and withdrawing rights and password changes;
e. security incidents, such as the presence of malware, tests for potential or actual vulnerabilities, login attempts, violations of authorization powers, blocked attempts to gain access, the use of non-operational system services, starting and stopping security management; and
f. disrupting the daily process, such as system errors, abortion during the execution of programs, non-availability of invoked program elements or systems.

8.4 VU Amsterdam ensures that the data that is collected through Logging is properly protected. This in any case means that:
a. the logging facilities and information in log files are protected against violations and unauthorized access;
b. adjusting, overwriting and removing log files – whether automatically or not – is logged in the newly created log; and
c. the log files can only be consulted by Authorized Officers. Access is limited to reading rights.

Article 9. Monitoring

9.1 VU Amsterdam only applies Monitoring if this is strictly needed to reach one or more justified objectives as stated in article 9.2. If alternatives are available with less privacy risks or other risks, VU Amsterdam shall prefer such alternatives or explain why these cannot be applied.

9.2 VU Amsterdam only applies Monitoring for the following purposes:
a. to prevent, identify and solve capacity, performance or availability problems of the ICT facilities;
b. checking whether the ICT facilities are used and managed properly and function properly;
c. to prevent, identify and solve security incidents, particularly Data Breaches;
d. to create 'evidence' (audit trail) to safeguard business operations, compliance with laws and regulations, and to be held accountable internally and externally about the use and security of the ICT facilities. The latter includes both external and internal audits and information provision to supervisory bodies such as the Dutch Data Protection Authority;
e. to issue management information as it relates to the confidentiality, integrity, availability and costs of the ICT facilities;
f. to improve the ICT facilities and access to them;
g. for scientific or statistical purposes, insofar as privacy laws allow it; and
h. monitoring compliance with these Regulations.

9.3 If Monitoring is required and no reasonable alternatives are available, Monitoring is only possible with due regard for the following conditions:
a. Monitoring takes place on a system-wide scale based on general parameters and patterns. In principle, no distinction is made per individual Staff Member; and
b. Monitoring is made known beforehand wherever possible in the context of information provision regarding that specific ICT facility, for instance via VUnet or via specific work instructions.

[4] The Traffic Data that are collected by means of Logging are only used for the purposes as stated in article 14.2. The data are not used to assess the individual performance of Staff Members or certain groups of Staff Members unless a written decision to this end has been taken by the Executive Board and the Works council. See also article 14.3.

CHAPTER 5. INDIVIDUAL INVESTIGATION

Article 10. Targeted and substantive investigation

10.1 Targeted Investigation is the starting point for investigations of an individual Staff Member. Only when it is clear that Targeted Investigation is insufficient to properly investigate the suspected conduct, a Substantive Investigation may be launched.

10.2 Targeted Investigation and Substantive Investigation are only possible when the following conditions have been met:

a. there is a justified suspicion of:
   - a violation of the Code of Conduct;
   - inappropriate conduct within the meaning of the Inappropriate Conduct Regulations of VU Amsterdam; or
   - another seriously culpable conduct of a Staff Member;
b. the targeted investigation is carried out by two Authorized Officers (four-eyes principle) under strict confidentiality;
c. a person authorized thereto has given written permission for the investigation. The order states the justified suspicion within the meaning of article 10.2 (a) and, in case of a Substantive Investigation, why a Targeted Investigation does not suffice. The order is given by the Director of Operations of the Faculty or the Director of the Service Department where the Staff Member concerned works, with the proviso that in the following cases only the Executive Board may give an order:
   - the Staff Member concerned is a Dean, Director of Operations or the Director of a Service Department;
   - the Staff Member concerned has a duty of secrecy, within the meaning of article 10.3 (b) or (c) or a confidential position within the meaning of article 10.3 (d); or

   - the investigation is carried out at the request of the complaints committee as referred to in the Inappropriate Conduct Regulations;

   The Executive Board or, if the Executive Board has given the order, the Supervisory Board, receives a copy of the order concerned at the same time. If the Staff Member is a member of Executive Board, the Supervisory Board of VU Amsterdam has given the order; and
d. the Staff Member concerned is informed as quickly as possible about the reason, execution and outcome of the investigation and is given the opportunity to provide further explanation. Information may be withheld from the Staff Member if disclosure could hamper the investigation. The principal of the investigation is informed about the postponement and the grounds for the postponement.

10.3 The following, additional rules apply to Substantive Investigations:

a. files and messages that have been marked as 'personal' are excluded from the investigation, unless there is a justified suspicion that they contain information about the suspected inappropriate conduct of the Staff Member;
b. if the Staff Member has a statutory duty of secrecy, all files and messages relating to the work of this Staff Member in that capacity are excluded from the investigation;[5]
c. if the Staff Member has a statutory duty of secrecy based on VU Amsterdam regulations, all files and messages relating to the work of this Staff Member in that capacity are excluded from the investigation, unless;
   - there is a justified suspicion that they contain information about the suspected inappropriate

[5] Staff Members with a statutory duty of secrecy include at least: occupational health physicians, psychologists, student psychologists and the Data Protection Officer (DPO).

conduct of the Staff Member; and
- the interest of the investigation in this case outweighs the interest that is served with the duty of secrecy in the relevant regulations;[6]

d. if the Staff Member has a confidential position that does not fall in the categories as referred to in article 10.3 (b) or (c), all files and messages relating to the work of this Staff Member are excluded from the investigation, unless there is a justified suspicion that they contain information about the suspected inappropriate conduct of the Staff Member[7];
e. privileged information pertaining to the Staff Member – including communications with an occupational health physician, psychologist, the Data Protection Officer (DPO), the Ombudsman, confidential counsellor and/or committee members as referred to in article 10.3 (c), the Works Council, the subcommittee, union consultants and lawyers – is excluded from the investigation, unless the suspected or established inappropriate conduct of the Staff Member directly relates to the contact with one or more of the persons and institutions referred to above.

10.4 The justified suspicion, within the meaning of article 10.2 (a), may be based on the outcome of Monitoring, Logging, own observations of VU Amsterdam and/or a report by a third party.

10.5 The data collected and the outcome of the Targeted Investigation and/or Substantive Investigation are only accessible – under strict secrecy – for the manager of the Staff Member concerned, the director of the faculty or department where the Staff Member works, the Executive Board, the members and the administrative secretary of the complaints committee, within the meaning of the Inappropriate Conduct Regulations, insofar as the investigation has been carried out at the request of this committee, and if applicable, the HR consultant and/or lawyer or employment lawyer involved for support. If the Staff Member concerned is a director or dean, the data collected and the outcome are only accessible – under strict secrecy – for the manager of the Executive Board, the members and the administrative secretary of the complaints committee, within the meaning of the Inappropriate Conduct Regulations, insofar as the investigation has been carried out at the request of this committee, and if applicable, the HR consultant and/or lawyer or employment lawyer involved for support. If the Staff Member concerned is a member of Executive Board, the data collected and the outcome are only accessible – under strict secrecy – for the manager of the Supervisory Board, the members and the administrative secretary of the complaints committee, within the meaning of the Inappropriate Conduct Regulations, insofar as the investigation has been carried out at the request of this committee, and if applicable, the HR consultant and/or lawyer or employment lawyer involved for support.

10.6 The outcome of a Targeted Investigation and/or Substantive Investigation are destroyed immediately if the suspected violation of the Code of Conduct and/or a seriously culpable conduct proves to be unjustified. The outcome is destroyed as soon as the need lapses to save it. The outcome of a Targeted Investigation and/or Substantive Investigation may be saved for longer if it is required for certain evidence at law or in the interest of a criminal investigation or report to the police.

Article 11. Objection against investigation

11.1 The employee who is the subject of a Targeted Investigation and/or Substantive Investigation, within the meaning of article 10, may lodge an objection against such investigation with the Executive Board within four weeks after being informed about the investigation.

11.2 The Executive Board shall respond in writing as soon as possible and in any event within four weeks after receipt of the objection, stating reasons for its decision. If the objection referred to in the preceding

[6] Staff Members with a prescribed duty of secrecy include at least: ombudsmen for staff and students, confidential counsellors and committee members in the context of the Inappropriate Conduct Regulations, the Whistleblowers' Scheme and the Scientific Integrity VU-VUmc Complaints Procedure.
[7] Staff Members in such confidential positions include at least: members of the Works council, members of the subcommittee, union consultants, student deans, academic advisors, staff welfare officers and editors of Advalvas.

paragraph is upheld, any data collected as part of the Targeted Investigation and/or Substantive Investigation is destroyed immediately. In addition, any measures will be repealed if they are proven to have been taken unjustly.

11.3 Lodging an objection does not affect VU Amsterdam from taking measures, within the meaning of article 12.

Article 12. Measures

12.1 VU Amsterdam retains the right to refuse Staff Members access to certain ICT facilities or limit their access to these facilities if the Staff Members act or have acted in violation of the Code of Conduct.

12.2 If a Staff Members is proven to have acted in violation of the Code of Conduct, the Executive Board may take appropriate measures against him or her, depending on the nature and severity of the violation, whereby dismissal – with immediate effect or otherwise – is the most far-reaching measure.

12.3 In case of an actual or justified suspicion of a criminal offence, VU Amsterdam might file a police report.

Article 13. Report to Works Council

13.1 The Executive Board reports annually to the Works Council about the number of individual investigations that have been carried out in a certain year, and the general outcome of these investigations. No data that can be traced back to individuals shall be shared.

CHAPTER 6. USE OF TRAFFIC DATA AND RETENTION PERIOD

Article 14. Use of Traffic Data

14.1 VU Amsterdam only uses Traffic Data in accordance with these Regulations.

14.2 VU Amsterdam only uses Traffic Data for:

a. Logging, as described in article 8;
b. Monitoring, as described in article 9;
c. an individual investigation, as described in chapter 5; and
d. following work processes. This includes a reminder–- automatic or otherwise – that is sent to a Staff Member when they do not perform a task in VUnet or not in time.

14.3 VU Administration does not use Traffic Data to assess the individual performance of Staff Members or certain groups of Staff Members unless a written decision to this end has been taken by the Executive Board and the Works Council has consented to it.

Article 15. Retention period

15.1 The data collected and processed in the context of Logging and Monitoring are not stored longer than required for the purposes for which they were collected and processed further.

15.2 VU Amsterdam complies with the statutory retention periods that apply to personal data and other data. Insofar as there is no statutory retention period, VU Amsterdam has established retention periods that can be found on VUnet.

CHAPTER 7. FINAL PROVISIONS

Article 16. Supervision

16.1 The Data Protection Officer of VU Amsterdam is charged with monitoring compliance with the provisions of these Regulations. VU Amsterdam shall ensure that the DPO is able to carry out their supervisory duties properly and independently. This means that the DPO receives no instructions on carrying out their duties from VU Amsterdam, including from the Executive Board, and that the DPO shall not suffer disadvantage from the performance of their duties. The VU DPO also advises the Executive Board.

16.2 All Staff Members are required to cooperate fully with the DPO within reasonable limits, unless a statutory duty of secrecy precludes such cooperation. Insofar as a duty of secrecy prevents a Staff Member from cooperating, the Staff Member will inform the DPO immediately.

Article 17. Implementation of new ICT system

17.1 Before the Executive Board proceeds to implement a new, important IT system, the Executive Board consults the Works Council about the implications in light of the provisions of these Regulations. In this context, the Works Council may have a right to deliver an opinion and/or a right to endorse, in accordance with the provisions of the Works Councils Act.

Article 18. Final provisions

18.1 In cases not provided for in these Regulations, the Executive Board takes a decision.

18.2 The Works Council has consented to these Regulations.

18.3 These Regulations are published on the VU Amsterdam website and on intranet (VUnet).

18.4 These Regulations were adopted by the Executive Board and entered into force July 2019.

18.5 The implementation of these Regulations are evaluated two years following its entry into force and discussed with the Works Council.

***