Wageningen University & Research – Network Regulations Governing Staff and Other Personnel (2022)

SUMMARY

Personnel (or many of them) need to use network facilities, equipment, software and data (hereinafter: the 'Facilities') within WUR[1] in order to carry out their work. However, their use involves risks. For this reason, WUR has drawn up a code of conduct that its personnel are expected to comply with when they use the Facilities. This code of conduct has been incorporated into these regulations.

These regulations govern the use of the Facilities by WUR's staff and other personnel (all of whom are hereinafter referred to as 'staff'). This also includes employment agency workers, self-employed individuals, seconded personnel, interns, visiting staff members and researchers, and internal and external PhD candidates. These regulations also apply to WUR staff's use of cloud services provided by other organisations through federated access. The personnel of other organisations that utilise federated access to WUR's cloud services are governed by their own organisation's regulations. The 'Wageningen University (WU) Network Regulations Governing Students (2021)' governs students' use of the Wageningen University Facilities. Where such a person is also a member of staff, the capacity in which they use the Facilities will determine which regulations apply.

WHAT IS ACCEPTABLE USE OF THE FACILITIES?

Whenever staff members use the Facilities that WUR provides to its personnel for the purposes of their work, staff members are required to comply with the WUR code of conduct in relation to data security, accessibility, the rights of WUR and any other parties, and the existence of appropriate conditions in the buildings and on the grounds belonging to WUR. This code of conduct has been incorporated into these regulations.

The following principles apply with regard to any use:

I) The Facilities will not be used for any activity in breach of the applicable legislation or public decency.

II) The Facilities will not be used for any activities that are harmful, pose a threat or are offensive to any other party.

III) The use of the Facilities will not compromise their availability, integrity or confidentiality (including any data held in them).

The above mentioned principles are set out in the form of a concrete code of conduct in these regulations. These regulations stipulate what amounts to the acceptable use of:

- any equipment that WUR makes available;
- the email and other electronic means of communication that WUR makes available;
- the internet access that WUR makes available;
- any equipment of their own that a staff member uses for the purposes of work they carry out for WUR;
- the use of Facilities that WUR makes available for personal purposes;
- social media;
- the protection of materials protected by intellectual property rights and confidential information (which does not constitute personal data).

[1] These network regulations apply to the personnel of Wageningen University and Stichting Wageningen Research. These two legal entities work together under the name of Wageningen University & Research (hereinafter: 'WUR').

How does WUR monitor the use and security of the Facilities?

WUR conducts inspections or arranges for other parties to do so to ensure that the Facilities are secure and available, and to enforce the rules stipulated in these regulations. In this respect WUR, seeks to achieve a healthy balance between the responsible and secure use of the Facilities and the relevant staff member's privacy. For this reason WUR ensures that any inspections that are conducted by or on behalf of it are proportional. The greater the risks and the more specific the indications of a breach, the more far-reaching and focused an inspection may be.

General monitoring

In the first instance, monitoring occurs automatically. This means data is monitored generally in such an aggregated way that it produces an overall picture of the use of all or part of the Facilities. Data that is traceable to an individual is only consulted if an automated alert constitutes grounds for doing so. Such data is only used for the purposes of verifying compliance with and the enforcement of these regulations. The data is deleted once it is no longer required for this purpose.

Focused investigation

Focused investigation occurs where the data of a specific staff member is recorded because there is a compelling suspicion that the staff member has contravened these regulations. For example, WUR may inspect the content of any communication or file in order to check whether there has been an actual breach.

What are the implications of breaching these regulations?

Where it is necessary to avoid any damage, the use of all or part of the Facilities may be blocked immediately. Should WUR detect a breach of these regulations, the staff member concerned will have an opportunity to explain their position before any move is made to adopt disciplinary measures. In addition to disciplinary measures, WUR may press charges in the case of a criminal offence and/or recover any loss that has been suffered as a result of the culprit.

How is the privacy of staff protected?

When enforcing these regulations, WUR complies with the applicable legislation and regulations, including the General Data Protection Regulation (GDPR). The personal data that WUR stores in response to any general monitoring or targeted investigation is secured appropriately. Only staff members who need to have access to such personal data – a very limited group – will have access to it. An attempt will always be made to collect as little personal data as possible to achieve the goals of these regulations. In those cases in which WUR processes personal data, as few people as possible will have access to it and it will be secured appropriately. The WUR Personal Data Protection Regulations govern personal data processing. Also see the lists of processed personal data pertaining to staff in and not in paid employment at the end of these regulations.

Contents

1. Purpose and scope of application

The code of conduct governing the use by WUR (hereinafter also 'the organisation') staff of the network facilities, equipment, software, and data that WUR makes available for their work (hereinafter 'the Facilities') is set out in these regulations. The potential implications of the application of these regulations for staff are also stipulated. By indicating what code of conduct applies in respect of staff who use the Facilities, WUR clarifies what acceptable use is in relation to:

- the security of systems and networks against loss or misuse, for example;
- the prevention of online and other forms of sexual harassment, discrimination and other criminal offences;
- the protection of privacy-sensitive information (including personal data);
- the protection of confidential business information;
- the protection of materials protected by intellectual property rights, including respect for the licensing arrangements that are applicable within WUR;
- the prevention of adverse publicity due to the unlawful use of the Facilities;
- the prevention of espionage;
- cost and capacity management.

These regulations apply to everyone who works for WUR when they use the Facilities that the latter has made available. As such, these regulations also apply to employment agency workers, self-employed individuals, seconded staff, interns, visiting staff members and researchers, and internal and external PhD candidates who have been deployed to carry out work for WUR. These regulations also apply if staff members secure federated access to other organisations' facilities in their capacity as a guest and staff members obtain such access using the login details of their own organisation. These regulations do not apply in the case of students. Separate network regulations have been drawn up for students for this purpose. In the case of staff who are also WUR students, both sets of regulations are applicable. In this case, the capacity in which the Facilities are used will determine which regulations apply.

Upon the commencement of employment or when an amended version of these regulations is adopted by the Executive Board, everyone will be afforded one opportunity to take cognisance of a summary of the content of these regulations by means of a pop-up window when logging in for the first time. Staff will be required to declare their consent before they may log in. Furthermore, staff will also have their attention drawn to the place where they may find the applicable version of these network regulations.

2. Use of the Facilities

In principle, WUR expects staff to assume responsibility for using the Facilities placed at their disposal in a way that does not breach the relevant legislation and regulations or social standards of decency. In this article, WUR sets out a concrete code of conduct that staff are expected to comply with when using the Facilities.

2.1. General

In order to use the Facilities, staff members will receive personal login details (a username, password and WUR passcode) and possibly additional means of authentication (such as a smart card or token). WUR expects staff members to exercise due care at all times with the login details and additional means of authentication given to them personally or which they have set for themselves. Personal login details and additional means of authentication must not be shared with any other party or reused outside the WUR domain. Should it be suspected that login details have been misused, WUR may take immediate action or even render the relevant account inaccessible.

WUR may prescribe or prohibit certain systems or applications for education, research and its operations, such as electronic learning environments, email systems, mobile or other applications, cloud facilities or multimedia services, such as messaging services. ApprovedApps can be found here. WUR encourages the use of applications featured in the ApprovedApps; it shows which data classification is suitable for which system. WUR expects staff to use the systems only for the purposes of providing education, conducting research, support processes and to ensure strict compliance with any limitations and requirements stipulated in this respect.

Software may be installed on equipment made available by WUR, where it is necessary for the purposes of carrying out work and provided that the relevant staff member may reasonably assume that the software is lawful and not harmful to the Facilities. Furthermore, the use of any third-party software that staff members installs themselves – hence not part of the software supplied by WUR – must comply with the applicable terms of use or licence at all times. A staff member or their manager will explicitly bear any risk or expense pertaining to a failure to comply with these terms. The consent of the relevant WUR service provider will be required in the case of any software that is not necessary for the purposes of performing staff members' work. Such service providers may only give consent, for example, by offering their core range of products. WUR intranet – equipment and software.

Active network components (such as access points, firewalls, routers and Wi-Fi printers) may not be connected without the network service provider's consent.

Access to WUR information from a network other than our own network facilities (from home, for example) is only permitted through a secure Wi-Fi or other network or a secure VPN made available by WUR for this purpose.
Furthermore, such information may only be accessed through equipment managed by WUR (a WUR client or My Workspace) or with staff members' own equipment, provided that it is actively managed and fitted with proper security stipulated by WUR (Link).

2.2. Use of email and other means of communication

Upon the commencement of employment, staff members will receive an email address, a telephone number and login details that they may use to log into the email system that WUR has made available. Furthermore, other systems supported by WUR may be supplied for the purposes of exchanging information. Such electronic means of communication are placed at staff members' disposal, as to enable them to perform their duties. Personal use is also permitted, subject to the terms and conditions stipulated in these regulations

When using electronic means of communication supplied by WUR (for personal purposes or otherwise), staff members are prohibited from:

- transmitting messages with pornographic, racist, discriminatory, threatening, insulting or offensive content (except where it is strictly necessary to do so for carrying out their work);
- sending messages with (sexually) intimidating content or any message that incites or may incite discrimination, hatred and/or violence;
- transmitting unsolicited messages to large numbers of recipients, chain letters or malicious software (such as viruses, ransomware or spyware).

What also applies specifically with regard to messaging apps, unless they are an enterprise version (business account) that WUR has explicitly approved and that therefore feature on the WUR applications[2] ApprovedApps, is that staff members are not permitted to use other

[2] MS Teams with a chat function, by way of example.

freely available electronic means of communication for the purposes of official WUR business for messages that:[3]

- contain the personal data of any staff member or student;
- concern policy formation and are subject to an archiving duty as well as a legal duty of disclosure;
- fall under the WUR data class of available, ethical or confidential and may be classified as 'singular', serious or disruptive. See the data classification link.

Should staff require a messaging app to communicate with external parties, for example, they are requested to use the MS Teams chat enterprise version (business account) or Signal (both of which are on the ApprovedApps) to exchange information that is not confidential.

In the event that a staff member is sick, absent, either unexpectedly or for a lengthy period, or is guilty of negligence, WUR may grant their replacement or superior access to their mailbox and work-related files. There must be a compelling business reason for granting such access, and the relevant staff member must be notified of this as far as is possible. No access may be granted to any folder marked as personal, email messages that are recognisable as personal or that have apparently been sent to or received from a confidential counsellor, an in-house medical officer or other physician, an HR advisor or anyone acting in the capacity of an attorney.

It is important that, where applicable, staff insert such designations in their mailbox and files. Where a staff member has not done this, WUR may call on a confidential counsellor to check the staff member's relevant information in order to identify personal information and set it aside before a replacement or the staff member's superior gains access.

After a staff member retires or dies, their account will be closed after two (2) weeks if possible, and any personal email communications or personal information on data carriers belonging to WUR will be destroyed.

2.3. Use of internet connection

Staff will have access to an internet connection provided by WUR in its buildings for the purposes of their work. As such, the use of an internet connection will, in principle, be linked to the work that follows from their position.

At any rate, whenever an internet connection provided by WUR is used, staff members are prohibited from:

- visiting websites that contain pornographic, racist, discriminatory, insulting or offensive material (except where this is necessary for the purposes of carrying out their work);
- using file-sharing or streaming services that generate excessive data traffic to the extent that this may endanger the availability of the Facilities;
- downloading or disseminating (sending or uploading) films, music, software and other protected (by copyright or otherwise) material to other parties, where the relevant staff member knows or may reasonably suspect that this infringes the intellectual property rights or other proprietary rights encumbering that material or an undertaking to protect the confidentiality of such material.

2.4. Use of the Facilities with the aid of personal equipment

Staff members may use their own equipment, such as smartphone, tablet or laptop computer, to carry out their work, provided that appropriate security measures have been adopted. Staff members are expected to adopt at least the following security measures:

- only use lawful software, which the supplier still actively supports;

[3] SMS and app such as WhatsApp, Signal, Teams, Telegram and so forth.

- protect the equipment with a password or a PIN code. Where possible, the relevant equipment may also be protected with face or fingerprint recognition;
- encrypt storage on the equipment;
- configure their equipment to lock itself automatically within five (5)minutes after leaving it unguarded, or lock the equipment themselves;
- store original information (or files containing same) for which WUR is responsible in the space provided for this purpose on WUR's servers;
- send files containing personal data through Teams or OneDrive only;
- store copies of information concerning WUR (or files containing same) in the latter's domain;
- keep software up-to-date by checking for and installing updates (at least once a month);
- adopt appropriate measures against viruses and malware by installing antivirus software, updating it and regularly scanning their equipment.

WUR reserves the right to check security measures, including the above-mentioned ones, for example with the aid of mobile device management (see Article 3.2.2). Upon the termination of their employment, staff members will be expected to remove any information for which WUR is responsible from their personal or other equipment.

2.5. Personal use of Facilities

Facilities may be placed at a staff member's disposal for them to use for the purposes of performing their duties. As such, their use is linked to the work that they perform in accordance with their position. They may only use the Facilities for secondary work, provided that WUR consents to this in writing.

Limited personal use may be made of the Facilities, provided that this does not disrupt day-to-day work or the availability or capacity of WUR's Facilities. Staff members may store a limited number of personal files or amount of information on equipment provided by WUR, provided that it does not breach the law or social standards of decency. WUR does not have a duty to make backup copies of such files or information, or to supply such copies if the relevant systems are replaced or repaired.

Supplying personal email correspondence or information on data carriers belonging to WUR or granting access to the email correspondence and information of a deceased person to their surviving relative(s) in some other way cannot be reconciled with the deceased party's integrity and the relevant correspondence partners' privacy interests.[4] It will only be possible to transfer any information that is requested – subject to certain guarantees – to a reliable, independent agency selected in consultation with WUR, which will assess that information and then request consent for its release from those correspondence partners. The applicant is required to engage this agency themselves and to bear the costs involved.

2.6. Use of social media

Staff are permitted to use social media for any matter that affects their work or position as WUR staff members. Nevertheless, staff are required to consider our good reputation and everyone involved. As such, use social media prudently and, when doing so, act in accordance with WUR's social media guidelines (link: https://intranet.wur.nl/umbraco/media/13562/richtlijnen-social-media-gebruik-door-medewerkers-op-eigen-accounts.pdf and https://intranet.wur.nl/umbraco/media/13558/richtlijnen-social-media-gebruik-offici%C3%ABle-accounts-wageningen-university-research.pdf.

[4] After all, it is important to respect the fact that no more may be revealed concerning such email correspondence than what the deceased and their correspondence partners themselves would have wished to reveal.

2.7. Dealing with confidential and privacy-sensitive information

Staff are required to treat confidential and privacy-sensitive information, including personal data to which they have access for the purposes of their work, in strict confidence and to adopt appropriate measures to ensure its confidentiality. Staff must only process information in systems that satisfy the requirements that WUR stipulates with respect to the category into which such information has been classified. Personal data is processed for the purposes of work for WUR in accordance with the WUR Personal Data Protection Regulations and the applicable policy based on them.

Control over WUR information is vested in WUR. Staff do not exercise any control over this information in their own right, unless WUR explicitly confers entitlement to do so on them.

Staff may not copy or download large numbers or substantial parts of articles taken from files or databases in the electronic library, unless this is required for the purposes of their work.

Where WUR has drawn up additional rules to secure the confidentiality and protection of material that is protected by intellectual property or other proprietary rights, staff will ensure strict compliance with them.

These provisions apply in the case of system administrators in particular, in respect of whom a failure to comply with them will be deemed to constitute grave dereliction of duty given their special position. Furthermore, all staff who are required to familiarise themselves with personal information for the purposes of oversight and monitoring in relation to these regulations are contractually bound to observe an additional duty of non-disclosure, except where any provision of the law renders such disclosure mandatory or the need for it follows from their duties.

3. Oversight and monitoring

This section sets out the way in which WUR will oversee compliance with these regulations and monitors its Facilities, and what measures may be adopted should these regulations not be complied with.

When overseeing and monitoring the Facilities, WUR will act in accordance with the applicable legislation and regulations, and the principles of necessity and proportionality. For the purposes of such oversight and monitoring, WUR will seek to adopt measures that confine access to privacy-sensitive information or personal data of individual staff members as far as possible. In this respect, WUR will act on the basis of an appropriate balance between the responsible use of the Facilities and the protection of WUR staff members' privacy. Where possible, WUR will pursue automated oversight or filtration without gaining an insight into the behaviour of individuals.

3.1. Conditions governing oversight

The use of the Facilities will only be overseen and monitored for the purposes of enforcing the rules set out in these regulations and solely for the purposes mentioned in Article 1.

3.1.1 Monitoring incidents

Monitoring and logging

In order to oversee any threats to the integrity, availability and confidentiality of WUR systems, all activities and information of all the users of the Facilities will be constantly processed automatically (monitoring and logging). Such logging data will be processed

using automated procedures, which may result in an alert being raised in accordance with predetermined rules.

Analysis of incidents
Only if it follows from the predefined rules that a system alert constitutes grounds for further investigation (for example, the detection of a virus or irregular login attempts) will the administrators of the relevant service and/or external or other analysts conduct further analysis of such alerts. Part of such an analysis may involve tracing an alert to a system or individual. This means that at that point in time, a WUR system administrator or external analyst may gain access to the nature of the information and activities of the relevant WUR staff member in so far as the alert concerns them (e.g. the content of a phishing message).

In an emergency or where required to ensure that a risk of harm does not materialise (or do so further), these staff members may decide to adopt technical measures, such as blocking access to a particular service or limiting the capabilities of the equipment in question to enable the network to be used. This will always involve temporary measures for no longer than the duration of the incident. Where the situation allows this, the information security officer (ISO) will assess whether the measure is appropriate in advance. In an emergency, the ISO will be notified as soon as possible after a measure has been adopted.

3.1.2 Monitoring an individual
Where WUR suspects that a staff member has contravened the rules, focused monitoring may occur for a stipulated (brief) period, and this may be logged as provided for in Article 3.1.1. Such monitoring will only focus on content should it appear that there are compelling reasons for doing so. The procedure for a targeted investigation is set out in Article 3.3.

3.2. Conducting general oversight
In order to oversee compliance with these regulations and to monitor the Facilities, WUR may adopt several specific measures, namely:

- Oversight to prevent adverse publicity and monitoring for the purposes of system and network security will occur on the basis of automated scans of content, such as email filtering and virus scanners.
- Oversight for the purposes of cost and capacity management. Where such sources result in major expenditure or inconvenience, they will be blocked or limited without infringing confidentiality with regard to the content of the relevant communications.
- Oversight to improve the security of the Facilities and to prevent the occurrence of cybersecurity incidents. For example, such oversight may occur with the aid of attack simulations (such as red team operations[5] and pen tests) and social engineering, such as phishing campaigns (see Article 3.2.1).
- The installation of mobile device management (MDM) software, which makes it possible to monitor certain behaviour and to render it impossible where necessary. Staff members may opt to use MDM to render their personal equipment suitable for performing WUR work (see Articles 3.2.2 and 3.3.).

3.2.1. Attack simulations and social engineering
In order to identify vulnerabilities it is necessary to conduct attack simulations and carry out social engineering on the Facilities or staff members' own equipment that is used to

[5] The purpose of red teaming is to reduce any risks and to improve the opportunities for WUR to adopt the appropriate and most efficient measures.

perform work for WUR. Such attack simulations and social engineering are only conducted in consultation with the ISO and with the latter's formal consent. In the case of social engineering privacy risks are also identified beforehand and are mitigated as far as possible in consultation with the data protection officer (DPO) with the help of a data protection impact assessment (also known as a DPIA).

Red teaming and pen tests are examples of such activities. Operations for the purposes of attack simulations and social engineering are carried out in line with the applicable privacy legislation. For example, personal data may be collected in the following ways in the case of attack simulations and social engineering:

- Social engineering: a user may be enticed to perform certain action or to surrender information, such as their password.
- Attack simulation: an attempt may be made to log into a device or system using an account with more privileges, thereby making it possible to view folders and files, potentially containing personal data and other information of a confidential nature.

Arrangements are made with the testing party doing this to ensure that any personal data that is found is dealt with in confidence. Any personal or other data that is found will not be stored for longer than is necessary for the purposes of the test. Personal and other data will be secured appropriately. Any folders or files which are explicitly designated as 'personal' will not be examined unless it is reasonably impossible to avoid this.

3.2.2. Mobile device management

Any equipment that WUR supplies or staff members' own equipment that is used to carry out work for WUR will be equipped with a mobile device management (MDM) agent. MDM makes it possible for WUR to manage matters centrally and in this way to improve security in relation to equipment and information and to eliminate risks, for example, those pertaining to serious data leaks. With the aid of MDM it is possible for WUR to conduct inspections or exert influence over equipment (and its use) in the following ways. Each option will only be utilised provided that it is necessary and proportional.

Staff members are required to ensure that their personal information is stored in a folder that is designated as personal, personal and confidential or a similar designation. WUR will not use MDM to inspect any folder that is designated as personal. WUR only monitors information that is not designated as personal. Nevertheless, in the case of a remote wipe, all personal information will also be deleted.

Any information that is obtained through the use of MDM will under no circumstances be used for any purpose (such as the assessment of the relevant staff member's performance) other than the availability, integrity and confidentiality of internal data.

3.3. The performance of targeted investigations

A targeted investigation occurs where traffic data or other information concerning a specific staff member is recorded and analysed to check whether any actual breach has occurred based on concrete indications within WUR of any breach of these regulations.

WUR may conduct a targeted investigation based on a compelling suspicion that a staff member has contravened these regulations. WUR will only conduct a targeted investigation after the Facilities and Services director issues written instructions to this effect and after obtaining advice from the CISO and the data protection officer (DPO), who will cite reasons as to why such instructions have been issued. The Executive Board will receive a copy of the instructions and an aggregated summary of the findings of the investigation. In the event that the advice provided by the CISO and/or the DPO differs from the instructions issued by the Facilities and Services director, the Executive Board will need to consent to the instructions to conduct an investigation in advance. Where an

investigation does not yield any grounds for additional measures, what has been recorded will be anonymised or destroyed.

Based on the concrete indications mentioned in Article 3.1.1, WUR may also conduct a targeted examination of the security or integrity of automated systems or peripheral equipment (such as routers or printers). In derogation from what is stated above, written instructions from the Facilities and Services director will not be required in this case.

A targeted investigation based on a compelling suspicion of a breach of these regulations will, in the first instance, be confined to the data obtained from logs that are already available, such as those of an individual user or system as mentioned in Article 3.1.1. Should a targeted investigation yield additional evidence, WUR may proceed to familiarise itself with the content of the relevant communications or saved files. This will again require the written consent of the Facilities and Services director in accordance with the procedure set out above, who will cite the reasons as to why consent has been granted.

The following are several specific personal measures that WUR may adopt for the purposes of oversight:

- Monitoring the leakage of confidential information. This occurs on the basis of random tests using keywords. Suspicious messages are put aside for closer investigation in consultation with the Executive Board.
- Checking for the prohibited use of email and other electronic means of communication. Two individuals will do this by opening electronic messages and consulting their contents based on a convincingly substantiated complaint. These individuals will be bound by a duty of non-disclosure in relation to the content.

The Facilities and Services director will notify any staff member who is suspected of contravening these regulations of the grounds for, the conduct and the findings of the investigation within three weeks. The staff member will be afforded an opportunity to explain their position concerning any information found. Such notice may only be delayed provided that it could actually undermine the investigation and only for the period that is necessary to take any disciplinary action. Advice will be obtained from the DPO beforehand.

Except in urgent circumstances or where there is a clear suspicion that these regulations have been breached, those WUR staff members who are directly responsible for overseeing and monitoring compliance with these regulations will only have access to the content of the relevant documents, email messages or other files provided that staff members have consented to this in writing. In that case staff members will be notified of the findings of the investigation afterwards.

3.4. Ensuring privacy in the case of oversight

WUR processes the personal data of the users of the Facilities when overseeing and checking compliance with these regulations and monitoring the Facilities. This may involve all of the personal data that is processed through the Facilities, including the content of work-related communications or saved files. When overseeing and monitoring at the level of personal data, WUR complies in full with the GDPR and other relevant legislation and regulations referred to in this article.

3.4.1. Measures for the purposes of privacy

Purpose limitation

WUR processes a staff member's personal data solely for the purpose set out in Article 1.

Accuracy

For the purposes of monitoring in relation to these regulations, WUR adopts any measures that are required to ensure that personal data is accurate and precise having regard to the purposes for which they are processed.

Data minimisation
WUR has structured the oversight procedure in such a way that the processing of personal data will remain confined to what is required for the purposes referred to in Article 1, amongst other things, by ensuring that the use of the Facilities will only be monitored through automated processing in the absence of any automated decision-making. Administrators and external or other analysists may only gain access to the content of staff internet, data and email traffic in the case of a concrete alert or a targeted investigation.

Storage limitation
Any personal data that is recorded for the purposes of overseeing and monitoring compliance with these regulations will be stored as briefly as possible. Only when there is a reasonable suspicion of unlawful use, may this period be extended for as long as is required to complete the investigation to be conducted in response. Once an investigation has been completed without it leading to disciplinary action against the person involved, the relevant information may be anonymised or deleted. Where an investigation does result in disciplinary measures, the relevant information will be stored as long as is necessary for evidential purposes or for the enforcement of disciplinary measures.

Integrity and confidentiality
In addition, WUR will adopt appropriate technical and organisational measures to secure any personal data recorded for the purposes of overseeing and monitoring compliance with these regulations against their loss and/or any form of unlawful processing. This may include the following measures, amongst others:

- WUR ensures, with the aid of technical, organisational and legal measures, that staff and external parties cannot gain access to the content of personal or other data except in so far as is stipulated in these regulations.
- Staff only have access to personal data where such access is required for the purposes of performing their work.
- Furthermore, all staff who are required to familiarise themselves with personal information for the purposes of oversight and monitoring in relation to these regulations will be contractually bound to observe an additional duty of non-disclosure, except where any provision of the law renders such disclosure mandatory or the need for it follows from their duties.
- WUR will periodically assess whether the administrators of the service comply with the arrangements that apply in relation to them with regard to authorisation, purpose limitation and non-disclosure when carrying out their work.
- WUR will periodically assess whether those parties with whom such data is shared comply with the arrangements that have been made.

3.4.2. Other parties
WUR will only share any information obtained through monitoring with another party if it is necessary to do so for the purposes of conducting an investigation and enforcing any disciplinary measures. As such, WUR may pass on such personal data to the police where a criminal offence is suspected or found to have been committed. Where WUR shares personal data with an external organisation, WUR will ensure that binding arrangements are made concerning the processing of such data by such an external party that at least satisfy the principles stipulated in Article 28 of the GDPR.

3.4.3. Confidential communications
Communications, such as email messages that are recognisable as having come from or having been sent to the members of a participational body, an in-house medical officer or other physician, the data protection officer, an HR advisor, a lawyer (acting in that

capacity) or anyone who may rely on confidentiality in accordance with the law, will not be inspected in the case of a targeted investigation based on a compelling suspicion of a contravention of these regulations. This will not apply in the case of general automated monitoring of security of email traffic and the network subject to the proviso that the content of such communications will not be viewed for the purposes of general automated monitoring.

3.4.4. Data subjects' rights, contact details and general provisions

The WUR Personal Data Protection Regulations govern personal data processing for the purposes of these regulations. Click here for more information about how WUR deals with personal data. The options for exercising rights under the terms of the GDPR can be found here.

4. Implications of breaching these regulations

In the event of a failure to comply with these regulations when using the Facilities, depending on its nature and gravity the Executive Board may take disciplinary action, block the Facilities or institute legal proceedings.

4.1 Disciplinary action

In the event of a failure to comply with these regulations or the generally applicable rules, depending on its nature and gravity the Executive Board may take disciplinary action. This includes a warning, reprimand, transfer, suspension and/or the termination of staff members' employment contract. Apart from this, the Executive Board may decide to limit access to certain Facilities temporarily or otherwise.

Disciplinary action may not be adopted (except as a warning) merely on the basis of the automatic processing of personal data, such as detection with the aid of an automatic filter or block (see also Article 4.2). Furthermore, no disciplinary action may be taken without affording the relevant staff member an opportunity to explain their position.

4.2 Blocking access to Facilities

Should a breach or suspicious behaviour be detected, WUR may block access to the relevant Facilities temporarily by automatic or manual means. Where the situation allows this, the ISO will assess whether the measure is appropriate in advance. In an emergency, the ISO will be notified as soon as possible after a measure has been adopted. Such a block will be maintained until it is shown that the cause has been eliminated. Should the cause be repeated, disciplinary action may be taken.

4.3 Pressing charges and compensation

Following documented consultation with the most appropriate disciplines within WUR, the latter may press charges at any time in the case of a suspected or detected criminal offence. Where WUR's assistance is requested in the case of a criminal investigation, it will provide such assistance in accordance with the law.

Acting at the Executive Board's behest, WUR may recover any loss suffered as a result of a contravention of these regulations.

5. Final provisions

In its capacity as an employer, under the law, WUR is entitled to adopt rules governing the performance of work and order in the workplace.

Because these regulations provide for the processing of personal data and monitoring of staff conduct and performance, there is a duty to obtain the consent of the relevant participational body on behalf of staff. This body consented to the substance of these regulations on February 28th 2022.

The Executive Board will, at any, rate evaluate these regulations every three years. Furthermore, WUR may amend these regulations with the relevant participational body's consent, should circumstances constitute grounds for doing so. Staff will be notified of a proposed amendment before it is introduced. The Executive Board will consider staff feedback before introducing an amendment.

In any situation that is not covered by these regulations, decisions taken by the Executive Board will be final.