REGULATIONS FOR USING THE DIGITAL NETWORK OF WAGENINGEN UR (WURnet)

1. Scope of these Regulations

1.1 These regulations apply to everyone who uses information technology (IT) facilities by means of the WURnet of Wageningen University (WU), the DLO Foundation and the Van Hall Larenstein Foundation (VHL), the framework of cooperation hereinafter referred to as Wageningen UR (University & Research centre).

1.2 WURnet is the collective name for all IT facilities of Wageningen UR; this includes the network itself, personal computers, servers, telephony apparatus and all other connected apparatus, including the corresponding software systems.

1.3 The supervision of the use of IT facilities via WURnet will be conducted in accordance with these Regulations, without prejudice to other applicable regulations, guidelines and codes of conduct, whether statutory in nature or enacted internally by/for Wageningen UR. The Supervising Authority is the Director of Facilities and Services (FB) of Wageningen UR, who acts on behalf of the Executive Boards of WU, DLO and VHL.

1.4 If a situation occurs which is not foreseen by these regulations, action will be taken in accordance with labour law, the Student Charter, the Personal Data Protection Act (WBP) and – regarding general aspects – in consultation with the Joint Representative Advisory Bodies.

2. Relevance and aim of these Regulations

2.1 These regulations concern general use and conduct rules that apply to all WURnet account users. WURnet account users are:

a. employees of Wageningen UR who, from a Wageningen UR workplace, use the IT facilities of WURnet referred to in Article 1.2. This subcategory also includes visiting staff members, seconded staff members, interns and temps;
b. students who, from a Wageningen UR workplace, use the IT facilities of WURnet referred to in Article 1.2.

These Regulations also apply to the use of the WURnet account if it is accessed from outside the workplaces of Wageningen UR.

2.2 The aim of these regulations is to create a proper balance between supervising and monitoring the responsible use of IT facilities and protecting the privacy and legal rights of WURnet account users. These Regulations therefore specify rules on how this use will be supervised and monitored.

3. Conditions and rules of conduct for using the IT facilities

3.1 The IT facilities, the storage capacity and the stored data are the property of the legal entities that form Wageningen UR. Access to WURnet is arranged by providing a strictly personal and non-transferable form of identification, which remains the property Wageningen UR. The combination of a user name and access code or other authentication facility that gives users access to the WURnet account is provided to the user by Wageningen UR under the obligation of confidentiality, with the following conditions and subject to the following rules of conduct.

3.2 Each user is individually responsible for correctly logging onto the Network and maintaining the confidentiality of the access codes provided by Wageningen UR or chosen by the user. However, granting permission to a third party to use the e-mail facility and agenda is permitted, if this is arranged via the existing WURnet account of this third party.

3.3 It is forbidden to use, commercially or otherwise, IT facilities for any objectives other than those related to the job duties or the study at Wageningen UR. IT facilities can be used for non-commercial ancillary activities if these activities have been approved by means of existing Wageningen UR procedures.

3.4 Users are forbidden from endangering the functionality of WURnet or hindering other users. The use of WURnet and all information systems operating on the network must always take place in such a way that their continuity, availability and integrity are not endangered.

3.5 It is forbidden to send undesired e-mail or to acquire the authentication data of other users and/or to use this authentication secretly.

3.6 Without written permission of the Supervising Authority, it is forbidden to connect apparatus to WURnet that do not comply with the connection standards. These can be obtained from the Servicedesk IT.

3.7 Users are forbidden to acquire non-authorised access to WURnet or to use software illegally. Users are deemed to report any weaknesses that are ascertained in WURnet to the Servicedesk IT.

3.8 With the exception of freeware, software on WURnet must not be copied for use on the IT systems of third parties. Users are forbidden to use the WURnet account to violate licensing rights or intellectual and/or industrial property rights.

4. Abuse of the provided IT facilities

4.1 Users must refrain from using WURnet to perform actions that could harm the reputation of Wageningen UR, or which are illegal or punishable by law. Subject to the rules of conduct referred to in Article 3, abuse is defined in any case as:

a. using WURnet to store and process illegally acquired information or information that is punishable to possess;
b. using WURnet to deliberately visit Internet sites or send e-mail messages that contain offensive (sexually intimidating), aggressive (racist), discriminatory or threatening material;
c. harassing other users of WURnet or hindering them in their activities by means of inappropriate behaviour;
d. revealing non-public information or services, which are stored in any form whatsoever on WURnet, to third parties without written consent of the owner;
e. using a security leak in WURnet to distribute, alter or delete software without permission;
f. using WURnet to place personal or commercial material on the Internet and/or to perform operations on existing material if these activities are unrelated to the job duties of the user;
g. Making WURnet accessible for commercial use or use by third parties.

Supervision protocol

5. General supervision by IT managers

5.1 IT managers[1] have, in principle, the same rights and obligations as other users of WURnet. However, due to their special position, IT managers have additional responsibilities.

5.2 Wageningen UR takes measures to ensure the position and integrity of the IT managers and/or the system administration department, as well as the supervision of these functions.

5.3 It is the task of IT managers to ensure that users have access to the hardware and software that they require for their activities. The IT managers treat information about the managed system and all information stored in the system that can be traced to individuals as confidential.

5.4 The IT managers are responsible for the system and network security of WURnet; they are also responsible for the installation and maintenance of the software on the network.

5.5 In case of a security incident, the IT managers can place temporary restrictions on the access to WURnet. Users are obligated to follow the instructions of IT managers.

6. Monitoring and registration

6.1 To monitor compliance with these Regulations, the Supervising Authority does not conduct systematic monitoring of e-mail traffic or the network and telephone traffic of users; in principle, the Supervising Authority limits this compliance monitoring to investigating traffic data that cannot be traced to individuals. As part of the technical management of the system and network, periodic copies are made of user and traffic information (log information). This information is never saved for more than six months.

6.2 In case of warranted suspicion of prohibited use, the traffic and user information (data about message originators, addressees, date, time, frequency and magnitude) will be stored until this is no longer necessary. Based on the provisions in the Personal Data Protection Act, prohibited use is reported to the Dutch Data Protection Authority.

6.3 The Supervising Authority, in case of security incidents (malware and spam) outside of normal malfunctions, can order the IT managers to investigate specific information (files, programmes) in order to solve the ascertained problems.

6.4 If required by corporate interest, and only under conditions where normal access to files via the user (employee) is impossible, the Supervising Authority, following written authorisation by the Executive Board, can secure files that were created as part of the employee's job duties.

[1] This includes telecom expense management

7. Targeted investigation

7.1 In case of warranted suspicion of violations of these Regulations, or in case of ascertained abuse as described – not exhaustively – in these Regulations, the respective Executive Board of WU, DLO and VHL reserves the right to order the Supervising Authority (in writing) to conduct a targeted investigation of the e-mail, network and telephone traffic of individual users.

7.2 In the cases referred to in Article 7.1, the Supervising Authority will conduct a targeted investigation that is initially limited to the relevant e-mail, internet and telephone traffic data, with the following aims:
a. Counteracting the improper and excessive use of IT facilities;
b. Monitoring compliance with agreements about the permitted and forbidden use of IT facilities;
c. Securing WURnet and monitoring whether corporate information is sufficiently protected and has not been made public.

Monitoring the personal details of e-mail, Internet and telephone traffic concerns the use of personal details as stipulated in the WBP.

7.3 If the Supervising Authority has ascertained that WURnet users have not complied with these regulations and/or are guilty of abuse, these users will be called to account for their behaviour as soon as possible by their manager or educational unit, and if applicable, will be given a statement in writing on the consequences if the ascertained behaviour or abuse is continued.

7.4 The Supervising Authority can conduct a targeted investigation of the content of e-mails only if there is a compelling reason to do so and following a written mandate by the Executive Board.

7.5 The Supervising Authority will not publicise the knowledge about the content, form and purpose of the messages and/or files of the users, to the extent this is not in conflict with the corporate interests of Wageningen UR and subject to the cooperation referred to in Article 7.7.

7.6 The party who is being investigated, as referred to in Articles 7.2 and 7.4, will be informed in writing immediately by the Executive Board regarding the reason for the investigation, its implementation and its result. The above party will be given an opportunity to explain the data that was found in the investigation. The provision of information to the above party will be postponed when further investigation is required.

7.7 Based on statutory provisions, Wageningen UR can be obligated to cooperate with providing information about the use of IT facilities by individual users of WURnet.

8. Measures

8.1 If an employee does not comply with these Regulations, the Executive Board can implement one or more of the following measures:
a. A temporary limitation of access to certain IT facilities;
b. A temporary or definitive ban on the use of certain IT facilities;
c. Other disciplinary measures as referred to in the applicable Collective Labour Agreements.

8.2 If an individual, as referred to in Article 2.1a, not being an employee, works at Wageningen UR and acts in conflict with these Regulations, the Executive Board, in addition to taking measures a–c, can also terminate his/her activities at Wageningen UR.

8.3 If a student acts in conflict with these Regulations, the Executive Board can take appropriate measures based on other regulations on the use of Wageningen UR buildings and other facilities. These regulations, to the extent they concern students, are based on Article 7.57h of the Higher Education and Research Act (WHW). Students can appeal against decisions made on these grounds to the Higher Education Appeals Tribunal.

8.4 If it is ascertained that a WURnet user has acted in violation of applicable provisions in criminal law, then this will be reported to the competent authorities. The user, manager or educational unit will be informed about this situation.

8.5 In case of violation of Articles 3 and 4, Wageningen UR can also claim damages from the user concerned by means of a civil lawsuit.

9. Final provisions

9.1 These Regulations go into force on 1 January 2011.

9.2 These Regulations can be amended with the approval of the Joint Representative Advisory Bodies. These amendments will be put down in writing and, before their enactment, will be announced to the users referred to in Article 2.1.

9.3 These Regulations will be evaluated once every three years with the Joint Representative Advisory Bodies.

9.4 These Regulations were enacted with approval of the Joint Representative Advisory Bodies by resolution of the Executive Boards of WU, DLO and VHL, on 13 December 2010.