The <Research Group> will act in compliance with the Personal Data Protection Act (2000), the EUR guideline on scientific integrity (1997), the EUR integrity code (2001). The <Research Group> will use the standard computer and network facilities of the Erasmus University Rotterdam (EUR) during the course of the research. See *Annex 1* for the *Regulations governing use of internet and it facilities for staff members at Erasmus University Rotterdam (2015)*.

Information Security Policy
The EUR CIO Office is responsible for establishing, issuing and monitoring the EUR Information Security Policy. The EUR Information Security Policy is based on *ISO 27002 Code of practice for information security management* with annual self-audits (ISO 27002), coordinated by the EUR Security Officer.

The EUR has appointed a Data Protection Officer as well as a Chief Information Security Officer to implement the General Data Protection Regulation[1].

The EUR Information Security Policy meets the standards and principles as defined in the Dutch National eGovernement Reference Architecture, commonly referred to as the *National Implementation Programme* (the i-NUP[2]) as well as the Dutch Higher Education Reference Architecture[3].

These measures contribute to the principles of Privacy by Design and Security by Design as currently adhered by the EUR.

For external communication and dissemination a <Research Group> public website will be made available as part of the standard EUR ICT services.

For internal communication, co-creation and file sharing, a <Research Group> intranet (secured access) will be made available. No public cloud services shall be used by the <Research Group> for data classified other than ´public data`.

ANNEX 1

REGULATIONS GOVERNING USE OF INTERNET AND IT FACILITIES FOR STAFF MEMBERS AT ERASMUS UNIVERSITY ROTTERDAM (2015)

The opportunity given to EUR Staff Members for using Internet and IT facilities (communications, computer and network facilities) placed at their disposal by Erasmus University Rotterdam (hereinafter: “EUR”) is generally an essential condition for such Staff Members to perform their work properly.

---

[1] In full: Personal data protection: processing and free movement of data (General Data Protection Regulation). See: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

[2] iNUP: http://www.e-overheid.nl/english

[3] NORA: http://www.wikixl.nl/wiki/hora/index.php/Hoofdpagina

However, use of such facilities may entail certain risks for EUR. In view of these risks, EUR is entitled to expect Staff Members to use the Internet and IT facilities in a responsible manner.

These Regulations are intended to lay down rules of conduct concerning the appropriate use of the Internet and IT facilities. In this connection, EUR's aim is to achieve a proper balance between safe and responsible use of the Internet and IT facilities as specified further in these Regulations, and Staff Members' privacy.

In addition, the Regulations devote attention to using the means of communication provided by EUR, such as telephones. Since using social media is of increasing importance, these Regulations also contain a few rules of conduct for using such social media.

As employer, EUR is entitled to set rules governing performance of work and a proper state of affairs on the shop floor. In addition, these Regulations are based on Article 1 paragraph 2 of the NU collective labour agreement. Since the Regulations provide for processing personal data and/or checking Staff Members' behaviour or performance, the EUR University Council (U-Council) and EUROPA have the right to endorse them.

These Regulations will come into force on 1 September 2015 after endorsement of these Regulations by the University Council dated July 14th 2015 and after endorsement by EUROPA dated August 18th 2015.

Article 1 - Definitions

In these Regulations, the following definitions are used for the following capitalised terms.

These definitions shall be interpreted as follows:

Administrator	The dean, director or head of the relevant section of the organisation at EUR.
Executive Board	The Executive Board of Erasmus University Rotterdam.
EUR	Erasmus University Rotterdam.
Hospitality Agreement	An Agreement in Writing between EUR and a natural person given the opportunity (under certain conditions) to perform work at EUR that is exclusively or to a predominant extent in their own interests, without any employment contract being concluded in this respect.

IT Facilities	Communications, computer and networking facilities at EUR, including telephone facilities, EURnet facilities together with all the relevant 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, and services offered to Staff Members which enable them to communicate on EURnet and networks connected to it.
Staff Member	A natural person who has or has had at least one appointment at EUR or at an institution that is part of EUR.

With respect to the scope of these Regulations, the Staff Members category will include all other natural persons who have signed a Hospitality Agreement, or who fulfil the following conditions:

they come under the category of persons as referred to in the University Data Model;
or: they come under the group of persons who also use the Hospitality Agreement in practice, or who have access to IT facilities as irregular staff members, e.g. temporary workers and trainees;
or: they come under the group of persons employed by the Holding and the operating companies.

Regulations The 'Regulations governing use of Internet and IT facilities for Staff Members at Erasmus University Rotterdam (2015)'.
In Writing Laid down in writing on paper or "by electronic means" as referred to in Book 6 Article 227a of the Dutch Civil Code.
System Manager A Staff Member possessing extensive powers in IT systems in connection with their administrative duties and their position.
Access Code The system comprising a user name or log-in name and the relevant (secret) authorisation code or password.

Article 2 - Starting points

These Regulations contain provisions concerning use of the Internet and IT facilities for Staff Members. The purpose of these Regulations is to establish a proper procedure in respect of the following:

system and network protection, including protection against damage and improper use;
combating sexual harassment, discrimination and other offences;
protecting personal data processed at EUR, e.g. that of EUR Staff Members, students and parents;
protecting confidential information, i.e. that of EUR, EUR Staff Members or Students;
protecting the intellectual property rights of EUR and third parties, including the respecting of licence agreements that apply at EUR;

preventing negative publicity;
cost and capacity control.

Limited personal use of the Internet and IT facilities is permitted insofar as this does not adversely affect Staff Members' work, is not disruptive to others, and does not adversely affect the proper functioning - including accessibility - of the network or other IT Facilities at EUR.
These Regulations apply to all persons in the Staff Members category as laid down in Article 1 of these Regulations. These Regulations do not apply to students enrolled in a bachelor or master programme at EUR, or to other natural persons who use the Internet or IT Facilities at EUR and who have not signed a Hospitality Agreement , including guest students or guest lecturers. The 'Regulations governing use of Internet and IT facilities for Students at Erasmus University Rotterdam (2015)' apply to this latter category of persons.
These Regulations likewise apply if use is made of other institutions' network facilities, whereby the EUR log-in data is used to access such facilities (eduroam).
In connection with enforcing these Regulations, EUR endeavours to take measures that restrict access to individual Staff Members' personal data as much as possible. Wherever possible, EUR will only carry out computerised checks or filters without allowing itself or others access to individual persons' behaviour.

Article 3 - Intellectual property and handling confidential data and information

Staff Members must treat confidential information, including personal data they can access in connection with their work, with the utmost secrecy and take appropriate measures to ensure that confidentiality is guaranteed.
Staff Members may not infringe the intellectual property rights of EUR and third parties, and must respect the licence agreements that apply at EUR.
EUR has control over all information of EUR. No Staff Member has independent control over this information unless EUR has explicitly assigned such control to them in Writing.
Staff Members must devote particular attention to taking measures as referred to in these Regulations if, in connection with performance of their duties, it is necessary to process confidential information, including research data and/or personal data, outside EUR such as in an e-mail, in non-institution-related cloud applications, on external storage devices or on their own equipment or storage devices, including USB sticks and tablets. EUR may set additional conditions regarding the admissibility and/or the way in which messages and files are stored, sent or shared. Staff Members must observe such additional conditions.
Staff Members must strictly comply with all regulations drawn up by EUR concerning the safeguarding of confidentiality.
The provisions of this Article apply in particular to System Managers, since breach of these provisions is deemed to be a dereliction of duty in view of the System Managers' exceptional position.

Article 4 - Use of communications, computer and network facilities

Communications, computer and network facilities are placed at Staff Members' disposal for use in connection with their position. For this reason, use should be connected with

work relating to this position. Personal use of these facilities is only permitted in accordance with the provisions of Article 2 paragraph 2 of these Regulations.
Staff Members are only permitted to use the facilities for commercial purposes other than those assigned by or for the benefit of EUR on condition that they have obtained the Administrator's consent in Writing, after consultation with the Administrator responsible for IT facilities at EUR.
The personal Access Code and any means of authentication assigned to Staff Members, such as smart cards and tokens, are strictly personal and may not be shared with others. Staff Members must treat the Access Code and all means of authentication with the utmost care at all times, and they are responsible for any use or further use made of these. Staff Members must take all reasonable measures to safeguard their Access Codes and all means of authentication. If a Staff Member discovers that these have been improperly used, they must immediately notify the System Manager thereof.
If improper use is suspected, the System Manager may decide to render the relevant account inaccessible with immediate effect.
In particular, Staff Members are not permitted to perform the following acts in respect of using the communications, computer and network facilities:

gaining access or attempting to gain access to other users' data and to programme files of computer systems, or altering or deleting these, unless consent in Writing thereto has explicitly been given;
gaining access or attempting to gain access to computer systems, insofar as such systems have not been created with explicit access options for Staff Members;
performing any acts that undermine the facilities' integrity and continuity;
attempting to obtain greater privileges for using the facilities than those assigned;
attempting to obtain system or user authorisation codes such as passwords, in any way or in any form;
reading, copying, altering or deleting messages intended for others, such as e-mails;
copying the programmes, databases and documentation provided by EUR or placing these at the disposal of third parties, unless consent thereto has been given in Writing;
introducing computer "viruses" on and through the IT facilities, either deliberately or by attributable acts and omissions.

Staff Members must comply with all general instructions for use of IT facilities issued by or on behalf of EUR. Staff Members must immediately comply with all instructions given by the responsible Administrator of the IT facilities at EUR during use of these facilities. EUR may set additional conditions and rules for use of the communications, computer and network facilities.
EUR may prescribe certain systems or applications for educational and other institutional purposes. If required, Staff Members must use the prescribed systems or applications when performing their work, and must strictly comply with the relevant restrictions and requirements set.
Installing software on the EUR IT facilities or otherwise adjusting or resetting the IT facilities such as adding a routing function, is only permitted after obtaining consent in Writing from the relevant Administrator, after consultation with the Administrator responsible for the IT facilities at EUR. EUR may set additional conditions to such consent. Staff Members must observe such additional conditions.
Staff Members may only connect their own equipment such as laptops, tablets or telephones to the wired and wireless network connections provided for this purpose. The Ad-

ministrator responsible for the IT facilities at EUR may set rules for accessing these connections for the purpose of enforcing these Regulations.
Staff Members are permitted to save a limited number of personal files and a limited amount of personal information on the EUR systems, provided that this does not result in overloading of these systems' storage capacity or disruption of the proper state of affairs on the shop floor. However, EUR is under no obligation to make back-ups of such files or information, or to make copies available in the event of replacement of or repairs to the relevant systems.

Article 5 - Use of IT communications and access to files

Personal use of IT communications such as e-mail and telephone is only permitted in accordance with the provisions of Article 2 paragraph 2 of these Regulations.
The e-mail system, together with the appropriate mailbox and e-mail address, are placed at Staff Members' disposal for use in connection with their position and are strictly personal. For this reason, use should be connected with work relating to this position.

The following acts are in any event strictly prohibited with respect to all use of communications, either personal or otherwise:

sending messages of a pornographic, racist, discriminating, threatening, insulting or offensive nature, messages that cause harassment or sexual harassment, and messages that might or would incite discrimination, hate and/or violence;
sending unsolicited messages to large numbers of people simultaneously, or sending chain messages or distributing malicious software (malware);

Staff Members should preferably refrain from using the e-mail address provided by EUR when sending personal messages. EUR will not block access to other e-mail services or specifically monitor this.
In the event of a Staff Member's illness, unforeseen long-term absence, dismissal, gross negligence or decease of the Staff Member, and unless it constitutes a compelling reason for access in respect of EUR's interests, EUR is entitled to allow a successor or manager access to the services where the files and e-mails are stored or to the Staff Member's mailbox.
Access to such files and e-mails or to a mailbox as referred to in paragraph 4 will only be granted after separate consent thereto has been obtained from the Executive Board. The successor or manager may not access files marked as personal, e-mails that are obviously personal, or e-mails sent to or received from a confidential advisor, occupational physician, HR counsellor or any other persons who may invoke confidentiality pursuant to the law. If the Staff Member has not marked any specific files or e-mails as personal, EUR will, where possible, opt to have an independent confidential advisor, who will be capable of identifying what information is personal, check the Staff Member's relevant information and move this information to a separate location before the Staff Member's successor or manager can access it. At the time the information is being accessed, a second person, appointed by the manager, will always be present, in addition to the successor or manager, to ensure the files and e-mails are dealt with scrupulously. In all situations where access is granted to the Staff Member's files or e-mails, this independent confidential advisor will, when possible, be informed.

E-mails from occupational physicians, HR counsellors, members of the University Council to each other and all parties who may invoke confidentiality pursuant to the law, will not be inspected. This restriction does not apply to computerised security checks carried out on the Internet and IT facilities.
EUR reserves the right to restrict access to certain telephone numbers. Such telephone numbers include those where the charges are very high.
Use of telephones provided by EUR will be registered. Such use is registered in connection with on-charging the costs of using telephones at EUR, and in order to safeguard the management, continuity, integrity and accessibility of the service or technical infrastructure. The actual content of telephone conversations will not be recorded.
In the event of exceptionally high telephone charges, EUR reserves the right to check the use of the telephone afterwards. To this end, EUR may request lists of telephone numbers and the duration of the calls made for each separate telephone. A targeted investigation as referred to in Article 9 of these Regulations may be carried out on the basis of the results.

Article 6 - Using the Internet

Access to the Internet and the appropriate facilities are placed at Staff Members' disposal for use in connection with their position. For this reason, use should be connected with work relating to this position.
Personal use of these facilities is only permitted in accordance with the provisions of Article 2 paragraph 2 of these Regulations.
The following acts are in any event strictly prohibited with respect to all use of the Internet, either personal or otherwise:

visiting Internet sites of a pornographic, racist, discriminating, insulting or offensive nature, or downloading this type of material;
using file sharing or streaming services if this generates a disproportionate amount of data traffic and thereby has a disruptive effect on the proper functioning of the network or other of the EUR IT facilities, including accessibility;
downloading films, music, software and other copyrighted material from any illegal source, or if a Staff Member is actually aware that this is a copyright infringement;
disseminating films, music, software and other copyrighted material among third parties or placing such material at their disposal without the copyright owners' consent;
unlawfully accessing non-public sources on the Internet;
deliberately altering or destroying information that others have accessed on the Internet without obtaining consent thereto.

Article 7 - Use of social media

EUR acknowledges the options for open dialogue, knowledge sharing and exchanging ideas between Staff Members, colleagues and other people on the social media. In the case of work-related issues, Staff Members must state EUR's name, their own name and their position at EUR, plus the fact that this is a personal opinion that does not necessarily correspond to that of EUR. Staff Members are obliged to behave in a manner befitting a good employee when using social media and posting comments on such media.

Administrators, managers and other persons who implement policy or strategy on behalf of EUR have a special responsibility when using social media, particularly if the content is related to their work.
This Article also applies if Staff Members use social media on their personal computers. However, it applies exclusively insofar as this concerns use that might affect their work.
If a Staff Member opens and/or manages an account on the social media that relates directly to their work at EUR even though it is opened personally in the Staff Member's own name, EUR and the Staff Member must seek an appropriate solution for transferring this profile and/or the information and contacts contained therein, on termination of the Staff Member's employment at EUR.

Article 8 - Monitoring and checking

Checks on use of the Internet and IT facilities may only be carried out in connection with the objectives referred to in Article 2 of these Regulations. Prohibited use of the Internet and IT facilities (if applicable) will be prevented by technical means as much as possible.
Computerised data may be compiled for checking compliance with these Regulations. This data is only accessible to the System Manager directly responsible, and in principle, it will only be placed at the disposal of other Administrators and similar responsible persons in anonymous form so that they can decide on additional technical measures.
In the event of suspicion of breach of the Regulations on the part of a Staff Member or a group of Staff Members, checks will in principle be restricted to individual traffic data level respecting use of e-mail and the Internet. The actual content will only be inspected if there is serious cause to do so.
Specific measures that EUR may take for inspection purposes include the following:

checks to prevent negative publicity and sexual harassment, or checks carried out in connection with system and network security. In principle, such checks are carried out on the basis of filtering the content for key search terms. Suspicious messages will be automatically returned to the sender;
checks relating to cost and capacity control. Such checks are limited to verifying sources of cost and capacity demand such as addresses for Internet radio and video sites, on the basis of traffic data. If using these websites results in considerable charges or nuisance, they will be blocked or access thereto will be discontinued without violating the confidential nature of the content of the communications;
checks based on complaints or reports by third parties concerning e.g. use of copyrighted visual material or random checks carried out on visual material available to the public.

Article 9 - Procedure for targeted investigations

Targeted investigations may be said to exist if traffic data or other personal information concerning a specific Staff Member is recorded in connection with an inquiry resulting from a serious suspicion of breach of the conditions and/or basic principles as laid down in these Regulations by this specific Staff Member.
Targeted investigations will only be carried out after the Administrator has given instructions for this in Writing. The Executive Board will receive a copy of these instructions and a report of the results of the investigations. If the investigations do not justify additional measures, the report will be destroyed.

As a departure from the preceding paragraph, targeted investigations into the safeguarding or integrity of peripherals will be carried out by the System Manager on the basis of specific indications. In such cases, no separate instructions in Writing from the Administrator are required. The relevant Staff Member will only be informed of the results of these investigations for the purpose of improving the safeguarding or integrity of peripherals. If the Staff Member repeats the offence, the procedure referred to in paragraph 2 of this Article will be followed.
In the first instance, targeted investigations are limited to traffic data concerning the use of Internet and IT facilities. If targeted investigations result in additional proof, EUR may decide to inspect the content of communications or saved files. Such an inspection requires the Executive Board's consent, which must be substantiated and in Writing.
Specific personal measures that EUR may take for inspection purposes include the following:

checking for leaks of confidential information. These will be random checks carried out using key search terms. Suspicious messages will be set aside for further investigation, in consultation with the Executive Board;
checking for violations of the prohibition referred to in Article 5 paragraph 3 of these Regulations must be carried out by allowing two persons to open e-mails and peruse the content on the basis of a specific complaint or random checks. These persons are bound to secrecy with respect to the content.

The Administrator responsible will inform the relevant Staff Member - in Writing and as soon as possible - of the reasons for the investigations, the fact that they have been carried out, and the results thereof. The Staff Member will be given the opportunity to explain the information revealed by the investigations. Informing the Staff Member may only be postponed if this would actually be deleterious to the investigations.
System Managers may only access Staff Members' computer accounts on condition that such Staff Members have consented thereto in advance. Accessing these accounts without such consent from the relevant Staff Member is only permissible in urgent cases, or if there is a clear suspicion that the Staff Member has breached these Regulations as stipulated further in this Article, or after obtaining consent thereto from the Executive Board in Writing. In such cases, the Staff Member will be informed afterwards.

Article 10 - Consequences of infringement

In the event of failure to follow instructions or directions on the basis of these Regulations and/or acting contrary to these Regulations or the generally applicable statutory regulations, the Executive Board may take disciplinary measures depending on the nature and gravity of the relevant offence. Such measures include in any event warnings, rebukes, transfer, suspension, and termination of the Staff Member's employment contract. In addition, the Executive Board may decide to limit access to certain of EUR's IT facilities and applications, either temporarily or permanently.
No disciplinary measures will be taken without first allowing the Staff Member the opportunity to put their own views forward.
Except for a warning, no disciplinary measures may be imposed if the investigations were only carried out on the basis of computerised processing of personal data, such as a discovery based on an automatic filter or blockade.

As a supplement to the foregoing, it is possible for EUR to implement a temporary blockade of the relevant facility in the event of any computerised or non-computerised discovery of nuisance. This blockade will be maintained until it has been demonstrated that the cause has been eliminated. If the cause is repeated, disciplinary measures may be taken.

Article 11 - Revoking of the former Regulations

These Regulations replace the 'Regulations governing use of computer and network facilities at Erasmus University Rotterdam (EUR)'.

Article 12 - Final provisions

These Regulations will come into force on 1 September 2015.
The Executive Board may amend these Regulations. Amendments may only be implemented at the start of an academic year, except in urgent cases or if external circumstances oblige EUR to implement them at an earlier date.
EUR may amend these Regulations if circumstances so demand. EUR will inform Staff Members of the proposed amendments prior to their implementation as far as possible.
The Executive Board will take feedback from Staff Members into consideration before implementing amendments.
The decision rests with the Executive Board in cases not provided for in these Regulations.
These terms are available in English. In the event of any conflicts, the Dutch text shall prevail.

————

English version: http://www.eur.nl/english/erna/information/users_information/use_-policy_employees/

Dutch version: http://www.eur.nl/erna/informatie/gebruikers_informatie/gebruiksreglement_medewerkers/