Integrity and behaviour code for ICT staff at UM

Date 1st version	Registration number	Author	Change management
20 October 2004	**ICTS/IS-2006-00124**	**Bart van den Heuvel, ICTS**	**Central Information Security Officer**
STATUS: Definitive Working instruction			
Distribution of document	**Draft: Administrative & Legal Affairs (BJZ), ICTS Management, DO-ICT; Decision-making: Coordinating Directors' Board (*CBB*), ICT portfolio holder; Implementation: Managements of administrative units who must declare the work instruction applicable / HRM officers; For information: LO list;**		

Version	Date	Description of change
0.1	**20 Oct. 2004**	**1st version, sent to BJZ for feedback**
0.2	**26 Nov. 2004**	**Modified in response to BJZ feedback**
0.3	**13 Jan. 2005**	**Modified in response to BJZ feedback, explanation moved to appendix**
1.0	**31 Jan. 2005**	**1st operational version, approved by Management and Services Council**
1.1	**8 March 2005**	**Language corrections**
2.0	**1 Sep. 2005**	**Draft modified to allow application of code throughout UM**
3.0	**6 April 2006**	**Modified for working instruction, implementation of Collective Labour Agreement (CAO) changes and termination of Campus@Maastricht facilities**
3.1	**27 sept 2006**	**art. 1.2 modified according to "mandatenregeling UM"**

DEFINITIONS

Information processing and information systems
Any form of processing or using any type of information and/or information systems.
Examples of processing:

- acquiring access to or obtaining;
- reading, copying or deleting;
- distributing in any form whatsoever (digitally, on paper, verbally, etc.).

Examples of information and information systems:

- digital data, system software and application software;
- voice messages, written materials, audiovisual material;
- resources of whatever type (computers, telephones, printers, fax equipment, photocopiers, mobile equipment, etc.).

Incident involving information, information security and the use of information systems
Every breach of confidentiality, integrity and availability or any threat thereof as well as any form of unallowable use of information and information systems or any threat thereof which directly or indirectly fall under the responsibility of the ICT staff of Universiteit Maastricht (UM).

Unallowable use
Any use of information and information systems in conflict with the job responsibilities of the person involved and the objective of the facilities, as well as activities in conflict with legal regulations, general agreements within UM or its administrative units, the Collective Labour Agreement (CAO) and agreements formulated in the Appendix "User regulations for MAASnet facilities UM", which is part of "CONDITIONS OF USE AND MANAGEMENT OF MAASnet UM".

Private use
Private use of information or information systems which is limited to generally accepted private activities within the framework of the terms & conditions and facilities of employment offered. The organisation or unit of the organisation may formulate additional rules of behaviour in this regard. An example would be the use of telephone and/or e-mail facilities to make appointments during office hours.

Integrity and behaviour code for ICT staff at UM

OBJECTIVE OF THIS DOCUMENT

This code is intended for ICT staff at UM and specifies how such staff are expected to deal with information which they process as part of their job responsibilities and with the information systems they use in doing so.
For several Articles, a further explanation is available in Appendix 1 of this document; these Articles are marked with (*).

GENERAL

Article 1

1.1 This integrity and behaviour code applies to ICT staff at Universiteit Maastricht and works out in more detail the Collective Labour Agreement of the Dutch Universities, *CAO-NU* (1 Jan. 2006 through 31 Aug. 2007), in particular Article 1.16 of the CAO-NU, the "CONDITIONS OF USE AND MANAGEMENT OF MAASnet UM" and any other relevant specific formal provisions within the organisation or unit of the organisation in which the person concerned is employed, such as house rules and regulations regarding private use of information systems.

1.2 Non-compliance with this integrity and behaviour code can lead to neglect of duty as defined in the CAO-NU (Article 6.12 CAO NU). A disciplinary measure may be implemented regarding ICT staff persons guilty of neglect of duty by the Executive Board.

1.3 For the purposes of this code, an ICT staff person is defined as:

1. every employee of Universiteit Maastricht with a job position belonging to the ICT job family (UFO);
2. the director and management staff of the organisation or unit of the organisation in which this employee is employed;
3. other persons who carry out ICT activities at/for UM under the supervision of a UM organisational unit;
4. other persons carrying out work activities at/for UM in support of the persons listed under 1, 2 and 3 and who therefore obtain or can obtain access to information related to the work activities of the above persons.

INTEGRITY

Article 2

Without prejudice to the provisions of this code, the ICT staff person is obligated to deal confidentially with information made available to him[1] within the framework of his job responsibilities to the extent that this obligation is explicitly applied to him or is evident from the nature of the information (*). This obligation remains in force after termination of the employment contract.

Article 3

The obligation referred to in Article 2 does not apply to those persons who, in view of their job responsibilities within UM, share responsibility for ensuring that the ICT staff person can properly carry out his work (*).

Article 4

In accordance with Article 12, section 1, of the Personal Data Protection Act, the ICT staff person processes the personal information to which he has access only at the request of the Executive Board or parties with an appropriate mandate, unless relevant legislation provides otherwise.

Article 5

In accordance with Article 12, section 2, of the Personal Data Protection Act, the ICT staff person is obligated to deal confidentially with the personal information which he becomes aware of within the framework of his job position, unless relevant legislation requires him to provide information or his job position requires him to provide information (*). This provision regarding confidentiality is an obligation based on a legal regulation as defined in Article 272 of the Dutch Criminal Code.

Article 6

Unless permission is provided by the individual employee or student concerned, the ICT staff person is not authorised to read documents or e-mails or to watch the use of other information systems by employees and students unless an investigation initiated as a result of an incident or unallowable use requires him to do so (*).

[1] In this document, the term ‘he/him/his’ is a gender-neutral description that includes ‘she/her’.

Article 7

The ICT staff person will carry out an investigation targeting an incident or unallowable use only if one or more of the workstations connected are/were involved in causing a serious nuisance or if the use of connected workstations or specific access codes were involved in or suspected of being involved in a serious threat. Such an investigation must be limited to information or information systems which fall under the direct or indirect management responsibility of the ICT staff person. In that case, the ICT staff person can actively investigate the status of usage or behaviour/network behaviour of the stations or users involved, register any such information and, if necessary, take measures to prevent any further misuse and/or limit any further threats.

If there are clear indications that improper use is being made of university information or information systems, an additional investigation may be carried out into the use of university information facilities by an individual employee or student. Such an additional investigation may be carried out only with permission from the Executive Board or the director of the ICT Service Centre with a mandate in that regard. The investigation must be carried out in accordance with the provisions in Article 5 of “CONDITIONS OF USE AND MANAGEMENT OF MAASnet UM”

Article 8

If during random general checks on information flows and/or the use of information systems or as the result of investigations carried out in response to incidents, information is obtained regarding the contents of documents or e-mails belonging to employees or students, the obligation to maintain confidentiality will not apply towards the Executive Board or parties with a relevant mandate.

BEHAVIOUR

Article 9

In carrying out practical work activities and, in particular, when using UM information systems and other UM ICT facilities, the ICT staff person will comply with existing legal guidelines (as set down, for example, in the Personal Data Protection Act, the Computer Crime Act, the Copyright Act, etc.) and the elaborations of these guidelines by UM, as well as the provisions in the "CONDITIONS OF USE AND MANAGEMENT OF MAASnet UM". (*)

Article 10

In carrying out his work activities, the ICT staff person will refrain from any behaviour which damages trust in UM or the organisational unit in which the staff person is employed on behalf of UM.

Article 11

The ICT staff person will take the greatest possible care in using information. This means that the staff person will take measures to prevent third parties from accessing information not intended for them. Point of departure is that, as a minimum, the following measures will be taken to that end:

- The systems used must be equipped with a form of access control which ensures that only those users authorised to do so can use the systems and/or data and that access to unauthorised persons is denied;
- The above implies that verification of user identity must be carried out, as a minimum, with the help of a user identification and a password. The passwords used must meet the general criteria for proper passwords, as formulated by UM;
- In order to prevent visual access by unauthorised parties, monitors must be set up in such a fashion that third parties cannot easily view the screen;
- In order to prevent misuse during periods of absence – including brief periods of absence – the staff person must ensure that during his absence no sensitive information is available to third parties on the system, preferably by logging out of the system or, for example, by activating a password-protected screen saver when leaving.

Article 12

The ICT staff person will do all that can be reasonably expected of him to safeguard the confidentiality, integrity and availability of the data present on the UM information systems to which he has access.

Article 13

The ICT staff person will immediately report any incidents or supposed incidents involving information or information systems of which he becomes aware to his manager. The manager is then expected to take appropriate measures to avoid similar incidents from occurring again.

Article 14

The ICT staff person must manage and maintain the workstations made available to him within the framework of his work activities in accordance with the guidelines formulated for such workstations. He will not carry out any modifications to the configuration unless they are necessary for doing his work. If modifications are needed which will result in expanding the standard communication protocols (network protocols, peer-to-peer networks, etc.), permission must be requested to do so from the operational manager of the workstations or from the manager.

Article 15

The ICT staff person will make use of the UM information systems and other UM ICT facilities only when it is necessary for carrying out his work. This includes all facilities for external access, such as dial-up, VPN and Proxy access.

Private use must remain limited to use which can be viewed as ‘Private use’ within the framework of the terms of employment. Such use must always be in compliance with the provisions set out in Articles 9 and 14 of this code.

Article 16

Every ICT staff person will be given specific authorities needed for carrying out his work activities, which are a direct result of the job responsibilities of that person. (*) The ICT staff person may not allow any other person to make use of these authorities.

Article 17

The use of specific authorities assigned to the ICT staff person applies specifically to that person’s work activities. These authorities may not be used for any purposes other than those resulting directly from the job description of the ICT staff person.

Article 18

If his job activities change, the ICT staff person is expected to inform his manager which changes must take place regarding his authorities. The manager must inform the operational manager of the system/subsystems involved of the desired and necessary changes.

Article 19

If the employment contract is terminated, the ICT staff person is expected to inform the manager of the specific modifications of authorities which were implemented for him and which therefore have to be modified upon his departure. The manager must inform the operational manager of the systems/subsystems involved regarding the necessary changes in authorities. The manager is also responsible for terminating the other general levels of authority of the departing ICT staff person (*). This releases the ICT staff person from any further responsibility for the confidentiality, integrity and availability of general or specific information and information systems.

Article

This code can be referred to as ‘Integrity and behaviour code for ICT staff at UM’.

Integrity and behaviour code for ICT staff at UM
Appendix I, explanation

APPENDIX I

Brief explanation of Integrity and behaviour code for ICT staff at UM

Article 2

The ICT staff person is expected to be able to determine, on the basis of the nature of the information, whether the information is confidential in nature. If necessary, the staff person can consult with his manager in this regard.

Article 3

This concerns ICT staff colleagues who are directly involved in the proper implementation of a specific task. The exchange of information is needed for properly carrying out the task concerned.

Article 5

This provides supplementary information with regard to the confidentiality of personal data, as there is specific legislation which applies to such cases. In Articles 2 and 3, the information involved may also be of a different nature. The inclusion of a reference to the Dutch criminal code introduces a framework for possible sanctions.

Article 6

Any such necessity can result from complaints (formal or otherwise), legal obligations, or threats/supposed threats evidenced by random samples or management information.

Article 9

This involves general behaviour demonstrated by the ICT staff person **himself**. The ICT staff person may not use any illegal software etc.

Article 16

This involves authorities not possessed by normal users or other ICT staff persons.

Article 19

Usually, the cancellation of general levels of authority will be taken care of via what is called a ‘general Exit’ procedure from the organisation or unit of the organisation. However, the manager remains responsible in this regard.