STELLENBOSCH UNIVERSITY

ELECTRONIC COMMUNICATIONS POLICY

1 December 2003

INDEX **Page**

Words defined in the definitions clause in Addendum A are underlined and printed in blue in this ECP. Please refer to the definitions clause in Addendum A for comprehensive explanations of these words. Addendum B contains excerpts from the relevant legislation. For the complete text of a relevant Act, please click on the reference thereto.

REMARKS REGARDING AMENDED LEGISLATION

Issues related to the interception and monitoring of communications were in the past regulated by the Interception and Monitoring Prohibition Act No. 127 of 1992. The South African Law Commission was however tasked with investigating possible amendments to this Act, in order to ensure that it complies with international standards and meets the requirements of the Constitution of the Republic of South Africa.

The Constitution in Section 14(d) states in this regard that every person has the right not to have the privacy of his or her communications infringed. However, as with any other constitutional right, this is not an absolute right in all circumstances, since Section 36 stipulates that rights may be limited to the extent that the limitation is reasonable and justifiable.

In a report published in November 1998, the Law Commission pointed to a number of shortcomings in the Act of 1992, particularly with regard to circumstances which would permit the interception and monitoring of communications.

As a result, the Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002 was assented to on 30 December 2002. Although the date of commencement of this Act is yet to be proclaimed, this will in all probability occur before the end of the year 2003.

The 2002 Act broadly prohibits the interception and monitoring of communications unless authorised by the aforesaid Act. In this regard Sections 5 and 6 expressly authorise the interception and monitoring of any communication if the parties concerned give their consent or if it relates to the running of a business, as the case may be.

Section 6 stipulates that any person may, in the course of the carrying on of any business, intercept in the course of its transmission over a telecommunication system any indirect communication -

- by means of which a transaction is entered into in the course of that business;
- which otherwise relates to that business; or
- which otherwise takes place in the course of the carrying on of that business.

.

The definition of the term "business" in the 2002 Act subsumes the activities of the University. The University is thus obliged to revise its current Electronic Communications Policy to accommodate changes in the regulatory environment, and has therefore decided to start revising its existing policy and at the same time address certain other operational matters and privacy issues.

1. INTRODUCTION

1.1 The use of the University's electronic communication Facilities is subject to its official Electronic Communications Policy (hereinafter referred to as "ECP") as set out hereunder, and any other relevant policy provisions and procedures of the University from time to time. If a User does not agree with this policy, he or she has no right to the use of these Facilities.

1.2 For purposes of the ECP it is assumed that a User -

1.2.1 is familiar with the provisions of Section 14(d) of the Constitution of the Republic of South Africa Act No. 108 of 1996, which protect the constitutional right to privacy, and that he or she fully understands these important provisions (the text of Section 14(d) is reproduced in full in Addendum B), and

1.2.2 therefore in terms of Section 14(d) of the Constitution and Section 5 of the Regulation of Interception of Communications Act No. 70 of 2002, consents to the privacy of such communication being infringed solely to such extent as may be necessitated and as authorised by the provisions of this ECP.

1.3 The policy provisions on Communications as contained in this policy document, and as amended from time to time in terms of paragraph 9, are by reference incorporated in the University's service conditions and/or the Regulations for Students, as the case may be.

2. ACCEPTABLE AND UNACCEPTABLE USE

2.1 The University shall permit reasonable use of all the Facilities of the University, provided that the University expressly reserves the right (for the purpose of its operational needs or as required by law) to:

2.1.1 review and, where necessary, restrict or suspend the User's access to and/or use of the Facilities by reason of and in accordance with the seriousness of the non-observance of the provisions of the ECP; and

2.1.2 recover from the User, on demand, the costs incurred during personal use, provided that costs of all use by a student may be recovered from such student in the absence of an agreement to the contrary.

2.2 The User shall not use the Facilities -

2.2.1 for the purpose of creating, sending or storing Communications which, in the discretion of the Rector or his nominee, may reasonably be seen to be disruptive, defamatory, discriminatory or sexually harassing to another person, or could lead to a breach of confidentiality;

2.2.2 in any manner which infringes upon another person's rights of personality or intellectual property rights (e.g. copyright);

2.2.3 for the purpose of making personal information in the possession of the University, which was obtained through the use of the Facilities, of any person known or available to a third party without the permission of such person;

2.2.4 in any manner which, in the sole discretion of the IT Representative, places an unacceptable burden on or disrupts the operation of the Facilities, including but not limited to any burden or disruption created by connecting to the Facilities, without prior consent, hardware or the installation of software that does not belong to the University;

2.2.5 for the purpose of violating the terms of any applicable telecommunications licence or South African laws governing cross-border data flow (e.g. legislation relating to data protection, privacy, confidentiality and security);

2.2.6 for the purpose of unlawfully accessing or attempting to unlawfully access the computer network or any electronic system of the University, or any other electronic system, or of gaining or attempting to gain unauthorised access to any person's computer, e-mail or voicemail facilities or equipment;

2.2.7 for the purpose of violating or attempting to violate any other applicable South African law, prescription or provision;

2.2.8 for the purpose of obtaining or attempting to obtain any Communications not intended for the User. The User shall in particular not attempt to Intercept or Inspect Communications transmitted or being transmitted, or stored, by means of the University's Facilities, or by means of any hardware connected to these Facilities, unless the information is intended for the User;

2.2.9 for the purpose of damaging, altering or attempting to alter the hardware and system configurations of the Facilities unless authorised to do so; and

2.2.10 in contravention of the terms in paragraph 3.3 with regard to the use of passwords.

2.3 The IT Representative may on request of any User exempt him/her from any limitation imposed in terms of paragraphs 2.2.4, 2.2.6 and 2.2.9.

3. USER'S RESPONSIBILITIES

3.1 The User shall be responsible for -

3.1.1 safeguarding passwords to, and any other security related information about, any Facility that has access to the University's network, whether permanently linked to such network or not;

3.1.2 taking reasonable precautions, including personal password maintenance and file protection measures, to prevent the unauthorised use of Facilities by other persons; and

3.1.3 using the Facilities only for the purpose for which the User has been authorised.

3.2 Reporting security incidents or network vulnerabilities

3.2.1 It may happen that the User may become aware of a breach or suspected breach of security with regard to the University's Facilities. Users are encouraged in every instance of this nature, to report such violation forthwith to one of the persons or organisations mentioned below:

3.2.1.1 the system administrator concerned or the CUA manager;

3.2.1.2 the IT Help Desk, or

3.2.1.3 the IT Representative or his or her nominee.

3.3 Passwords

3.3.1 The User's passwords verify his or her identity in the electronic environment. Passwords used to gain access to the Facilities have to be kept confidential.

3.3.2 In highly exceptional cases, and if rendered essential by operational needs, group accounts may be created with the prior written authorisation of the IT Representative and passwords used accordingly. All the parties who have legitimate access thereto shall in turn keep the passwords to such group accounts confidential.

3.3.3 With regard to individual accounts, the User shall not at any time or for any reason use a password or username belonging to another person, not even with express permission, provided that a User may allow another

User (without disclosing or making available any passwords) right of access to his or her electronic accounts.

3.3.4 The User shall be responsible for logging off open sessions of the Facilities, where applicable, if any such systems are left unattended for any length of time. Should the User fail to comply with the aforesaid responsibility, he or she shall be held responsible for any activities that may take place under his or her username as a result of such failure. This additional responsibility shall include, without limitation, any account or damage that may arise from the said activities.

4. THE ECP AND THE RIGHT TO PRIVACY

4.1 The University respects the User's right to privacy as that right is guaranteed by the Constitution. Yet in the context of the University's Facilities, which are provided for the purpose of the operational needs of the University and of Users, restrictions on the User's rights in certain defined circumstances, as herein contained, are nevertheless unavoidable.

4.1.1 The University will attempt, within reason, to implement a detailed policy on privacy by no later than 1 January 2006. Such policy shall, *inter alia*, regulate the purpose and extent of, and limitations to, the University's use and disclosure of personal information about Users.

4.1.2 The present ECP will be revised, if necessary, after the implementation of the policy on privacy.

4.1.3 The University's criteria with regard to the application of filtering software will be published.

4.2 All Facilities owned or controlled by the University shall within reason be accessible for -

4.2.1 maintenance;

4.2.2 upgrades;

4.2.3 system-driven monitoring actions aimed at countering or minimising the loss of personal data; and

4.2.4 any other such lawful operational or related purposes for which prior written authorisation have been given by the IT Representative.

4.3 Although the University respects the User's right to privacy as set out in paragraph 4.1 above, the University is obliged to manage and protect its communication systems, and the person authorised thereto in terms of paragraph 5 may, therefore, without further notice to the User (but subject to paragraph 5), Intercept, Refuse or Inspect any Communication in the exercise of the University's responsibility for the operation of its Facilities. Such action shall only be instituted on the ground of one or more of the following objectives:

4.3.1 to ensure that the University's Facilities are not being used in contravention of paragraph 2.2;

4.3.2 to determine the presence of illegal material or unlicensed software;

4.3.3 to implement system-driven anti-virus software and install systems for the control of junk e-mail;

4.3.4 to counteract crime;

4.3.5 with a view to institute or for use during or in response to legal proceedings requiring such Communications to be produced or disclosed;

4.3.6 with a view to institute or for use during or in response to a disciplinary hearing and/or investigation,

4.3.7 to investigate potential transgressions of legislation or the University's procedures, policies and/or codes of conduct; or

4.3.8 to establish and/or perform the University's rights and obligations to third parties.

4.4 The User hereby gives his or her express consent that the University may, as provided by clauses 4.2 and 4.3 only, Intercept and/or Refuse and/or Inspect all Communications.

4.5 The User furthermore, also gives his or her specific express consent that the University may disclose any Communication-related Information that has a bearing on a Communication that may rightfully be Intercepted, Refused or Inspected in accordance with the ECP, for the purpose of the aforesaid lawful Interception.

5. INTERCEPTION CONTROLS

5.1 An Interception may be effected by the IT Representative only, or by a person designated for this purpose from time to time and duly authorised thereto, in writing, by the IT Representative.

5.2 Any Interception of the User's Communications regarding the Division for Information Technology's compliance of its duty to ensure the effective and proper functioning of the University's IT infrastructure, shall be subject to prior review and written authorisation by the IT Representative and may include:

5.2.1 scanning for viruses and other harmful software;

5.2.2 investigating possible security breaches; or

5.2.3 Refusal or Interception of junk e-mail.

5.3 All Interceptions related to any alleged transgression of:

5.3.1 a South African law, or

5.3.2 the University's disciplinary code and/or rules for students, as the case may be,

or any other Interception that cannot be authorised in terms of paragraph 5.2, is subject to the prior review and written authorisation of the Legal Advisor or his or her nominee, provided that the Legal Advisor or his or her nominee is convinced that reasonable grounds exist for such Interception. The Legal Advisor must, when

deciding if an authorisation must be granted, consider less infringing alternatives to Interception, if available.

5.4 The Legal Advisor shall keep a detailed record of all the Interceptions authorised by him or her in terms of paragraph 5.3, indicating inter alia the following:

5.4.1 particulars of the applicant;

5.4.2 the purpose and extent of the Interception;

5.4.3 the time period of the Interception; which shall not exceed 90 calendar days, and

5.4.4 the names of those persons to whom written authorisation had been given by the IT Representative to effect the Interception.

The same particulars shall be furnished in the authorisation referred to in paragraph 5.3.

5.5 The Legal Advisor shall submit an annual report to the Rector and his or her Management team, of statistics on such Interceptions as were authorised by him or her in the course of the previous year. Such statistics will be presented in such a way that individual persons will not be identifiable therefrom and will be made available for inspection in the office of the Registrar.

5.6 Any information obtained from an Interception shall be confidential and may not be stored or used for any purposes other than those authorising the Interception in the relevant paragraph or clauses.

5.7 The Legal Advisor shall, after an authorisation was issued in terms of paragraph 5.4, notify the designate personnel representative in the case of a member of the personnel, and the designate student representative in the case of a student, of the purpose and extent of the Interception, the duration thereof and the number of times an authorisation is issued in respect of a specific person. The aforementioned representative shall be nominated annually in writing by the University's personnel organisations and the Student Representative Council

respectively. The aforementioned representative shall at all time keep the information furnished to him or her confidential and may only provide the said information to the Ombudsman or authorised third parties (i.e. in terms of a court order) for further investigation.

6. CONSEQUENCES OF VIOLATION

Violation of any of the provisions of this policy shall be construed as misconduct and may result in one or more of the actions mentioned below:

6.1 the restriction, suspension or termination of the User's access to the Facilities, including the summary suspension of his or her access or rights pending further investigations;

6.2 the institution of legal proceedings by the University, including but not limited to criminal prosecution under applicable laws that may prevail in South Africa from time to time, and

6.3 the taking of disciplinary steps against the User, which may lead, *inter alia*, to his or her suspension or dismissal.

7. COSTS

7.1 The University provides certain Facilities at prescribed rates, which rates are payable by the User (in the event of the User's department or division failing to effect timeous payment of such rates). By accepting the terms of this ECP:

7.1.1 the User authorises the University to recover from the User all monies payable by the User in this regard, and

7.1.2 the User undertakes to pay on demand the amount owing.

7.2 The User authorises the University, in the event of a failure to pay on demand any amount thus owing, to recover such amount from his or her remuneration, or to debit the User's student account with such amount, as the case may be.

7.3 It is the User's personal responsibility to remain constantly informed of the costs of the use of the Facilities, which costs may be adjusted from time to time after reasonable notice to the User.

8. INDEMNITY

8.1 The User indemnifies the University and its employees, agents and independent contractors, as the case may be, in respect of any loss or damage suffered by the User, including but not limited to the loss of data or damage to hardware or software, or the non-availability of systems or communications. Such indemnity shall not apply in cases where the University is shown to have been guilty of gross negligence or malicious conduct.

8.2 The User indemnifies the University and its employees, agents and independent contractors, as the case may be, and holds them harmless in respect of any claims instituted by third parties as a result of any transgression of the ECP by the User.

9. AMENDMENT OF ECP

9.1 Changes in legislation, operational needs and/or other relevant factors may from time to time require that this policy be amended.

9.2 An *ad hoc* forum consisting of representatives from, *inter alia*, formal employees' organisations and student bodies, as determined by the Rector, shall investigate and recommend amendments to this policy.

ADDENDUM A

DEFINITIONS AND INTERPRETATIONS

In this agreement, unless inconsistent with or expressly otherwise indicated by the context, the following definitions shall apply:

"Communication" shall have the same meaning as *"Communication*", as defined in the Regulation of Interception of Communications and Provision of Communication-related Information Act (No. 70 of 2002) and as it may apply to the Facilities of the University, including stored communications and data, and ***"Communications"*** shall have a corresponding meaning;

"Communication-related Information" shall have the same meaning as *"Communication-related Information"*, as defined in the Regulation of Interception of Communications and Provision of Communication-related Information Act (No. 70 of 2002);

"Facilities" means, without limitation, the following: telephones (landline telephones, mobile telephones and voicemail facilities); electronic mail facilities; facsimile machines and modems; computers and network tools and applications (including Internet access facilities and Web browsers) that belong to the University, are operated or provided by the University, or whereto the University controls access;

"Inspect" means the same as "Interception", and ***"Inspected"*** shall have a corresponding meaning;

"Interception" shall have the same meaning as "interception" as defined in the Regulation of Interception of Communications and Provision of Communication-related Information Act (No. 70 of 2002), and ***"Intercept"*** shall have a corresponding meaning;

"IT Representative" means the Senior Director: Information Technology, Stellenbosch University, or his or her nominee;

"Legal Advisor" means the Head: Legal Services, Stellenbosch University, or his or her nominee;

"Rector" means the Rector and Vice-Chancellor of Stellenbosch University;

"Refuse" means the system-driven return of a Communication to its sender without making it available or passing it on to the intended receiver, and ***"Refusal"*** shall have a corresponding meaning;

"University" means Stellenbosch University;

"User" means any person registered as a user of, or otherwise uses the Facilities of Stellenbosch University, including employees, contract workers, independent contractors, temporary appointments, visiting and seconded staff, students and alumni, and

"Written authorisation" includes authorisation that is issued electronically.

ADDENDUM B

EXCERPTS FROM THE RELEVANT ACTS

1. **Section 14(d) of the Constitution of the Republic of South Africa, Act Nr. 108 of 1996:**

"14. *Everyone has the right to privacy, which includes the right not to have-*

(d) the privacy of their communications infringed."

2. **Section 36 of the Constitution of the Republic of South Africa, Act Nr. 108 of 1996:**

*"**36. Limitation of rights***

(1) The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including-

(a) the nature of the right;

(b) the importance of the purpose of the limitation;

(c) the nature and extent of the limitation;

(d) the relation between the limitation and its purpose; and

(e) less restrictive means to achieve the purpose.

(2) Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights."

3. **Definitions in terms of the Regulation of Interception of Communications and Provision of Communication-related Information Act (No. 70 of 2002)**

"*communication*" includes both a direct communication and an indirect communication;

"*communication-related information*" means any information relating to an indirect communication which is available in the records of a telecommunication service provider, and includes switching, dialling or signalling information that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and, where applicable, the location of the user within the telecommunication system;

"*intercept"* means the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the-

(a) monitoring of any such communication by means of a monitoring device;

(b) viewing, examination or inspection of the contents of any indirect communication; and

(c) diversion of any indirect communication from its intended destination to any other destination,

and "***interception*"** has a corresponding meaning;

4. **Sections 4, 5 & 6 of the Regulation of Interception of Communications and Provision of Communication-Related Information (Act 70 of 2002):**

"4 Interception of communication by party to communication

(1) Any person, other than a law enforcement officer, may intercept any communication if he or she is a party to the communication, unless such communication is intercepted by such person for purposes of committing an offence.

(2) Any law enforcement officer may intercept any communication if he or she is-

(a) a party to the communication; and

(b) satisfied that there are reasonable grounds to believe that the interception of a communication of another party to the communication is necessary on a ground referred to in section 16 (5) (a),

unless such communication is intercepted by such law enforcement officer for purposes of committing an offence.

5 Interception of communication with consent of party to communication

(1) Any person, other than a law enforcement officer, may intercept any communication if one of the parties to the communication has given prior consent in writing to such interception, unless such communication is intercepted by such person for purposes of committing an offence.

6 Interception of indirect communication in connection with carrying on of business

(1) Any person may, in the course of the carrying on of any business, intercept any indirect communication-

(a) by means of which a transaction is entered into in the course of that business;

(b) which otherwise relates to that business; or

(c) which otherwise takes place in the course of the carrying on of that business,

in the course of its transmission over a telecommunication system.

(2) A person may only intercept an indirect communication in terms of subsection (1)-

(a) if such interception is effected by, or with the express or implied consent of, the system controller;

(b) for purposes of-

(i) monitoring or keeping a record of indirect communications-

(aa) in order to establish the existence of facts;

(bb) for purposes of investigating or detecting the unauthorised use of that telecommunication system; or

(cc) where that is undertaken in order to secure, or as an inherent part of, the effective operation of the system; or

(ii) monitoring indirect communications made to a confidential voice-telephony counselling or support service which is free of charge, other than the cost, if any, of making a telephone call, and operated in such a way that users thereof may remain anonymous if they so choose;

(c) if the telecommunication system concerned is provided for use wholly or partly in connection with that business; and

(d) if the system controller has made all reasonable efforts to inform in advance a person, who intends to use the telecommunication system concerned, that indirect communications transmitted by means thereof may be intercepted or if such indirect communication is intercepted with the express or implied consent of the person who uses that telecommunication system.