NWU® | Information Technology

Private Bag X1290, Potchefstroom
South Africa 2520

Tel: +2718 299-1111/2222
Fax: +2718 299-4910
Web: http://www.nwu.ac.za

RULES AND GUIDELINES FOR THE PROTECTION OF IT INFRASTRUCTURE AND THE USE OF COMPUTER FACILITIES

1 Introduction

The University provides a **Communication Network** and **Network facilities** (computer and networking facilities) to students, researchers, lecturers, support personnel and other stakeholders (hereafter called the user) for the execution and improvement of their work in a productive and cost-effective way.

This can be achieved only if the facilities are correctly used and are not abused, disrupted or damaged in any way.

2 Definitions

The **Communication Network** is the interconnection of two or more nodes for the purpose of data, video and voice transmission on the different campuses (LAN), between campuses (WAN) and outside the University. The media of transmission include copper, fibre-optic, radio, microwave, Bluetooth and infrared, among others.

Network facilities are any services that are used or made available through the **Communication Network** for other nodes, for example: fileservers, ftp, Gopher-server, bulletin-board, WWW-server, telephones, Internet, Peer-to-Peer, etc.

3 Conditions of use

Staff and students of the University have free access to information on a myriad of topics. The University's computer and network facilities provide access to information on local, national and international databases and networks.

When the University approves someone as a user, the University and the user enter into a mutual contractual relationship of trust in terms of which the University obtains power of control over the activities of the user. In terms of this contractual relationship, the user further authorizes the University to perform monitoring in certain circumstances. Such monitoring power justifies an infraction of the privacy of the user. However, such power does not extend unchecked and there are strict internal prescriptions it has to comply with.

4 Rules and guidelines

Under the definitions of **Communication Network** and **Network facilities**, the University prescribes the following rules and guidelines:

- Any intentional or negligent action that impairs the availability or usability of the **Communication Network** and the provided **Network facilities** is prohibited.

The following are prohibited:

- The intentional and/or negligent distribution of **computer virus**es or the development of such viruses;
- The additional supply of **Network facilities** on the **Communication Network** without the written consent of the Chief IT Director;

- Changes to, or expansion of the **Communication Network** without consent from IT. In other words, the connection of any equipment (including network interface cards, radio networking equipment and so forth) to the **Communication Network** of the University without approval by IT is prohibited. Network equipment or cabling may only be changed and/or extended by IT;

- The relocation of computer equipment to another room, building, house or hostel that does not comply with the Asset Control Rules. IT must be informed via an "IT-Help" request when computers or networking equipment need to be relocated;

- The usage of network protocols other than IP (TCP/IP) on the University's data network;

- Changes to the standard IP-setup as prescribed by IT;

- Smoking, drinking and eating in the computer laboratories. These must always be kept clean;

- Removal or uninstallation of any standard security software as prescribed by IT for the protection and management of the network facilities (i.e. Antivirus, WSUS, etc.);

- The use of Peer-to-Peer network facilities as available under the W indows Operating system;

- The running or usage of any radio network - even within the unlicensed radio spectra - on the property of the University without the consent of the Chief IT Director - irrespective if the link such networks may have with the University network or not;

- Intentional violation or attempts to circumvent the **security** of any **network facility** or **information system**. This implies, among others, access to or attempts to gain unauthorized access to the following:

    - Servers on which a user is not registered, except in the event of servers that host generally available information services (like bulletin-boards, campus-wide information, anonymous ftp, etc.);

    - Storage areas, except on the user's own computer, that has not been allocated or t o which access has not been explicitly granted by IT;

    - Obtaining or using another user's password without permission. The credentials of another user (personnel and postgraduate students must obtain written permission from the relevant head of department to use another user's credentials. Undergraduate students may not, under any circumstances, log in using other person's credentials);

    - Development or ownership or possession of programs with which passwords may be obtained or guessed;

    - Attempts to change another person's password using his ID-card;

    - Ownership of software with which encrypted documents may be decrypted;

    - The tapping or otherwise unauthorized monitoring of network traffic on any network (including telephone and radio networks) and the unauthorized possession of software or hardware that is designed to tap or monitor network traffic;

    - Intentional or negligent distribution of information that compromises the security of the computer and network facilities is prohibited. This implies, amongst others:

    - Disclosure of usernames to colleagues, friends or family members without the written consent of the relevant head of department; and/or announcement or documenting of passwords without the written consent of the relevant head of department;

    - Disclosure of email address lists without the consent of the Chief IT Director.

5 Ethical rules of use of the Communication Network and facilities

The use of the computer and network facilities for activities unrelated to the official work, duties and activities of the University, and which does not adhere to the ethics that may be derived from the foundation and character of the University, is prohibited. Among other things, this implies that:

- Users may not use the University's facilities for personal financial gain or the personal financial gain of others;
- No computer games may be played on any official computer of the University, except when this is assigned to students by a lecturer for purposes of training;
- No anti-Christian, immoral, pornographic and other morally corrupting information may be collected or made available on computer;
- No undesirable e-mail, for example unapproved general e-mails, may be sent. Email is an official communication medium and you may only use it for work and study-related purposes.
- Violation of copyright or plagiarism by means of or with regard to the computer or network facilities is prohibited. This implies, among other things, that the following are prohibited:
    - The use or possession of unlicensed software;
    - The provision of software without the authorisation of the copyright holder.

6 User responsibility regarding rule violations

- The user undertakes that the University will be **indemnified** from any damages suffered and costs or fines incurred by the University as a result of the users' contravention of any of the rules.
- Deviation from any of the stated rules may only occur with written authorisation from the Chief IT Director.
- In accordance with the University disciplinary regulations, disciplinary action can result from the transgression of these rules and/or action for damages the University may suffer as a result thereof.
- Reimbursement by the user for any damages suffered and/or costs or fines incurred by the University could result as outcome of the disciplinary process.

7 Rule exceptions or permitted deviations

- Deviation from any of the stated rules may only occur with written authorisation of the Chief IT Director.
- These rules are subject to change with the approval of the Chief IT Director and with proper notice to users.