PROVINCE OF KWAZULU NATAL

DEPARTMENT OF EDUCATION

Executive Information Security Policy Employee Declaration

Introduction

The purpose of Information Security is to protect the organisation's information assets from all types of threats whether internal or external, deliberate or accidental. Information Security Policy indicates management's commitment to Information Security, and the requirements needed to manage and mitigate these risks.

This policy applies to all employees of KZNDEC. Any user of KZNDEC resources must consent to all the provisions of this policy and agree to comply with all of its terms and conditions and any amendments, which may be made thereto by KZNDEC from time to time.

When a personal computer is connected to an enterprise wide network, it is transformed into an enterprise network device. Indiscriminate changes to the software and hardware can disrupt the functionality of the entire KZNDEC network, through the transmission of unwanted protocols, and the propagation of viruses etc. This will result in a burgeoning of the Total Cost of Ownership, which refers to the cost related to the maintenance of the IT infrastructure within KZNDEC. The costs within KZNDEC can only be contained if all users adhere to strict policies and procedures.

Data Confidentiality

The business software provided shall be used solely for KZNDEC business activities. All KZNDEC data produced with this software remains the sole property of KZNDEC and may under no circumstances be copied, reproduced or removed from any KZNDEC machine or premises.

Standard Business Software

All standard software (e.g. Microsoft Office, Outlook, etc.) shall be licensed in the name of KZNDEC and be installed by KZNDEC recognized I.T. personnel.

Specialised Software

Any component requiring specialised software shall in all cases consult the designated manager responsible for Information Technology about the use of such software, and should only be installed with the knowledge and/or support of the Information Technology committee. This is to ensure that additional software required does not conflict in any way with the standard business software.

Specialised software shall be licensed in the name of KZNDEC or be freely licensed software.

Prohibited Software

Non-business software (e.g. games, fancy screen savers and greeting card products, disk maintenance utilities, Internet tools, etc.) is not to be installed or run from any device attached to the KZNDEC network system. A software inventory project has been undertaken between November 2000 and January 2001 and management has taken steps to ensure that all installed software is appropriately licensed. Unauthorised software installed after the process will be the responsibility of the user and thus contravention could result in the user being penalised by the Business Software Alliance (BSA)

Copies of Copyrighted Software

Copies of copyrighted software on KZNDEC's network, computers or any storage media (i.e. floppy disks and tapes) are not allowed unless such copying is consistent with third party license agreements and is being made for contingency planning purposes.

Private Use
Software licenses in the name of KZNDEC shall not be installed on any non-KZNDEC owned computer. In such circumstances KZNDEC should apply through the normal channels for any additional licenses required.

E-mail and Internal Use
E-mail services, including mail addresses and accounts associated with these services are provided to authorised users primarily in support of KZNDEC's business activities. Any other Internet services are provided to authorised users for KZNDEC business only. KZNDEC personnel may not use the e-mail or Internet in any way that may tarnish the public image of KZNDEC. This applies particularly to the internal and external circulation of chain letters, jokes etc. Where it is felt that information of this nature has relevance to KZNDEC personnel, the authority of the Head of Department must be obtained before distributing such information. All other e-mails, particularly racist and pornographic type material is not permitted and should be deleted immediately. KZNDEC reserves the right. Where deemed appropriate, to review any files that pass through KZNDEC network.

All e-mail services and other Internet services provided remain the property of KZNDEC and KZNDEC reserves the right to:

- wholly or partially restrict the use thereof without prior notice and without consent of the user when there is substantiated reasons to believe that violations of policy or law have taken place
- withdraw such service at any time

Password
Passwords are the key to all the services offered on the KZNDEC network and as such are the first and favourite entry point for would be 'hackers' Passwords therefore should:

- be kept a secret
- be protected from misuse
  Under no circumstances be shared
- be of an acceptable length (minimum 6 alpha/numeric characters that would not be easily hacked)
- not be stored in drawers, on "post-its" or easily detectable places
- be periodically changed (at least monthly)

Modems
Modems may not be attached to computers in the local area network, except if expressly allowed by IT management. This restriction applies equally to laptop computers using PCMCIA type modems.

Virus Protection
A computer virus is an unauthorised software program that has been introduced into a computer system or network. The purpose of a virus is to damage files, "eat" space, delete data, and in some cases damage hardware. Virus protection software should automatically be used on all data entering and leaving the KZNDEC environment. Virus protection software is loaded on all Networked P C,s to validate is regularly updated to offer maximum protection.

The ways to protect your computer are to ensure that:

- All computers be scanned at least once a day
- Always ensure that latest version of the virus scan software
- Scan all files before installing new software is loaded
- Scan all files downloaded from the Internet
- Scan all files transferred via disks

- Refer all suspected viruses to the IT department, particularly those from suspicious origins

If you have any doubts or questions about your role in virus protection, please contact your IT manager.

Desktop PC's
Always exit from all applications and the network before going home for the evening and never leave the PC unattended for any length of time (lunch hours etc.) Use password-protection or lock the terminal when leaving the computer unattended.

END