Title: ***Standards and Guidelines for Desktop Computers***

Purpose:

Author
Marc Wilson
ICT Technician
Rose Bruford College

Technically Approved

Quality Approved

Authorised

Administration
Marc Wilson

Ref No *|projects|0001R|draft|sg_desktops.doc*
Version No *1.2*
Issue No *Issued*
Date Issued *27 June 2005*

Rose BRUFORD COLLEGE - Information Systems Technology

TABLE OF CONTENTS

1 Desktop Computer Security Guidelines

1.1 Definition

Desktop computers are personal workstations that, though possibly linked to other computers via a Local Area Network, function as stand-alone units. Desktop computers include IBM-compatible PC's, Macintoshes, and Unix Workstations.

1.2 General Obligations

Users and custodians of Desktop computers are subject to the "Conditions of Use" and "Code of Practice" specified in the College's IT Security Policy.

1.3 Hardware Security

- Lock offices. Office keys should be registered and monitored to ensure they are returned when the owner leaves the College.
- Secure Desktops in public areas. Equipment located in publicly accessible areas or rooms that cannot be locked should be fastened down by a cable lock system or enclosed in a lockable computer equipment unit or case.
- Secure hard disks. External hard disks should be secured against access, tampering, or removal.
- Mark personal computers clearly with the name of the owner.
- Locate computers away from environmental hazards.
- Store critical data backup media in fireproof vaults or in another building.
- Register all College computers.

1.4 Access Security

- Utilize password facilities to ensure that only authorized users can access the system. Where the Desktop is located in an open space or is otherwise difficult to physically secure then consideration should be given to enhanced password protection mechanisms and procedures..
- Password guidelines:
  - *(i).* Length should be at least eight characters.
  - *(ii).* Avoid words found in the dictionary and include at least one numeric character. (Six-character passwords may suffice for non-dictionary words.)
  - *(iii).* Choose passwords not easily guessed by someone acquainted with the user. (For example, passwords should not be maiden names, or names of children, spouses, or pets.)
  - *(iv).* Do not write passwords down anywhere.
  - *(v).* Change passwords every thirty days.
  - *(vi).* Do not include passwords in any electronic mail message.

1.5 Data and Software Availability

- Back up and store important records and programs on a regular schedule.
- Check data and software integrity.
- Fix software problems immediately.

1.6 Confidential Information

- Encrypt sensitive and confidential information where appropriate.
- Monitor printers used to produce sensitive and confidential information.
- Overwrite sensitive files on fixed disks, floppy disks, or cartridges.

1.7 Software

Software is protected by copyright law. Unauthorized copying is a violation of College Copyright policy. Anyone who uses software should understand and comply with the license requirements of the software. The College is subject to random license audits by software vendors.

1.8 Viruses

Computer viruses are self-propagating programs that infect other programs. Viruses and worms may destroy programs and data as well as using the computer's memory and processing power. Viruses, worms, and Trojan horses are of particular concern in networked and shared resource environments because the possible damage they can cause is greatly increased. Some of these cause damage by exploiting holes in system software. Fixes to infected software should be made as soon as a problem is found.

To decrease the risk of viruses and limit their spread:

- Check all software before installing it.
- Use software tools to detect and remove viruses.
- Isolate immediately any contaminated system.

1.9 Computer Networks

Networked computers may require more stringent security than stand-alone computers because they are access points to computer networks.

While IT Services has responsibility for setting up and maintaining appropriate security procedures on the network, each individual is responsible for operating their own computer with ethical regard for others in the shared environment.

The following considerations and procedures must be emphasized in a network environment:

- Check all files downloaded from the Internet. Avoid downloading shareware files.
- Test all software before it is installed to make sure it doesn't contain a virus/worm that could have serious consequences for other personal computers and servers on College networks.
- Choose passwords with great care to prevent unauthorized use of files on networks or other personal computers.
- Always BACK-UP your important files.
- Use (where appropriate) encrypting/decrypting and authentication services to send confidential information over a College network.
- Never store College passwords or any other confidential data or information on your laptop or home PC or associated floppy disks or CD’s. All such information should be secured after any dialup connection to the College network.

END OF DOCUMENT.

RESPONSIBILITIES:

Custodian	MARC WILSON
Monitoring Officer	UNCONTROLLED
Information Contact	INFORMATION SYSTEMS TECHNOLOGY

RELATED PUBLICATIONS / POLICIES :

"STANDARDS AND GUIDELINES FOR STRATEGIC SYSTEMS"
"STANDARDS AND GUIDELINES FOR ALL USERS OF COLLEGE COMPUTING AND NETWORK FACILITIES"
"INFORMATION TECHNOLOGY SECURITY POLICY"
"STANDARDS AND GUIDELINES FOR SCHOOL-BASED SYSTEMS"

Document Number	DRAFT / UNCONTROLLED	**Revision Number**	1.0
Document Location	\\SERVER01\ICT$\PROJECTS\0001R\DRAFT		
Approved Date	DRAFT	**Approved by**	